2013-1419, -1420

United States Court of Appeals for the Federal Circuit

SL SERVICES, LLC

Plaintiff - Appellant,

v.

CITRIX SYSTEMS, INC. AND CITRIX ONLINE LLC

Defendants – Cross Appellants.

Appeal from the United States District Court for the Eastern District of Texas in Case No. 08-cv-158, Judge J. Rodney Gilstrap.

INITIAL BRIEF OF DEFENDANTS – CROSS APPELLANTS CITRIX SYSTEMS, INC. AND CITRIX ONLINE LLC

J. ANTHONY DOWNS
LANA S. SHIFERMAN
GOODWIN PROCTER LLP
53 State Street
Boston, MA 02109
(617) 570-1000

WILLIAM M. JAY
GOODWIN PROCTER LLP
901 New York Avenue, N.W.
Washington, DC 20001
(202) 346-4000

ERICA D. WILSON
DAVIS WRIGHT TREMAINE LLP
505 Montgomery Street, Suite 800
San Francisco, CA 94111-6533
(415) 276-6500

BLAIR MARTIN JACOBS
MCDERMOTT WILL & EMERY LLP
500 North Capitol Street, N.W.
Washington, DC 20001
(202) 756-8000

LEIGH JOHN MARTINSON
MCDERMOTT, WILL & EMERY LLP
28 State Street
Boston, MA 02109
(617) 535-4000

Counsel for Defendants-Cross Appellants Citrix Systems, Inc. and Citrix Online LLC

December 23, 2013

FORM 9. Certificate of Interest

UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

SSL Services LLC v. Citrix Systems, Inc. and Citrix Online LLC

No. 2013-1419, -1420

CERTIFICATE OF INTEREST

Counsel for the (petitioner) (appellant) (respondent) (appellee) (amicus) (name of party)

Cross-Appellants Citrix Systems, Inc. & Citrix Online LLC certifies the following (use "None" if applicable; use extra sheets if necessary):

1. The full name of every party or amicus represented by me is:

Citrix Systems, Inc. and Citrix Online LLC

2. The name of the real party in interest (if the party named in the caption is not the real party in interest) represented by me is:

Citrix Systems, Inc. and Citrix Online LLC

3. All parent corporations and any publicly held companies that own 10 percent or more of the stock of the party or amicus curiae represented by me are:

Citrix Systems, Inc. has no parent corporation, and there is no publicly held company that owns 10% or more of Citrix Systems, Inc.'s stock. Citrix Online LLC is a 100% wholly-owned subsidiary of Citrix Systems, Inc.

4. ☑ The names of all law firms and the partners or associates that appeared for the party or amicus now represented by me in the trial court or agency or are expected to appear in this court are:

Prior representation at trial court: J. Anthony Downs, Lana S. Shiferman, Thomas F. Fitzpatrick, Andy H. Chan, Laurel A. Kilgour, Ryan J. Thompson, Joseph R. Farris, Gerald P. Dodson, Steven D. Tang, D. Stuart Bartow, and Christl Denecke of Goodwin Procter LLP; Erica D. Wilson, of Davis Wright Tremaine LLP; Jennifer Parker Ainsworth, of Wilson Robertson & Cornelius P.C.; and Neil J. McNabnay and Carl E. Bruce, of Fish & Richardson. Expected to appear in Federal Circuit: J. Anthony Downs of Goodwin Procter LLP and Erica D. Wilson of Davis Wright Tremaine LLP.

May 28, 2013
Date

/s/ J. Anthony Downs
Signature of counsel

J. Anthony Downs
Printed name of counsel

Please Note: All questions must be answered
cc: _____

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

CASES

STATUTES AND RULES

OTHER AUTHORITIES

STATEMENT OF RELATED CASES

Defendants-Cross-Appellants ("Citrix") state that no other appeal in or from the same civil action in the lower court was previously before this or any other appellate court; and counsel is not aware of any case that will be directly affected by this Court's decision in this appeal.

GLOSSARY

Selected Claim Terms & Constructions

"virtual private network" ("VPN")	"a system for securing communications between computers over an open network"
"session key"	"a sequence of bits that is input into an encryption algorithm to encrypt data for a session"
"mutually authenticate"	"a server verifies the identity of the client computer and the client computer verifies the identity of the server"
"a shim"	"software that is added between two existing layers, which utilizes the same function calls of the existing layers"

Abbreviations & Other Terms

AG	Access Gateway
GoTos	Collectively, GoToMyPC, GoToAssist and GoToMeeting
NDI	Network driver interface
OS	Operating System; software arranged in levels or layers, together referred to as a "stack."
RFC 1508	Request for Comments 1508, "Generic Security Service Application Program Interface" by J. Linn (Sept. 1993)
Takahashi	"Communication Method with Data Compression and Encryption for Mobile Computing Environment" by Takahashi et al.
TDI	transport driver interface

STATEMENT OF JURISDICTION

The district court had jurisdiction over this case pursuant to 28 U.S.C. §§ 1331 and 1338(a). The district court entered judgment on the jury's verdict on September 17, 2012, A64-65, and denied the parties' post-trial motions on April 17, 2013, A66-100. Citrix filed a timely Notice of Appeal on May 17, 2013. A4370-4373. Citrix's cross appeal is from a final order. This Court has jurisdiction over Citrix's cross appeal pursuant to 28 U.S.C. § 1295(a)(1).

INTRODUCTION

These cross-appeals concern two related patents, each asserted against different Citrix products and services, and each raising different issues.

In its appeal, SSL challenges the jury's verdict that Citrix's three GoTo subscription services do not infringe the '796 patent. SSL contests three parts of the district court's claim construction and argues it was prejudiced by the court's failure to adopt SSL's alternative constructions. In each instance, the court's construction is correct. First, the court found that a "destination address," in the context of a claim covering transmissions between computers on "an open network," was a "network address" of a computer. It correctly rejected SSL's attempt to strip out the word "address" by construing "destination address" as merely an "identifier for a desired destination." Second, the court correctly construed the term "intercepting" in light of the patent's repeated definition of "the

invention" as the use of a "shim" (*i.e.*, special software inserted between "layers" in a computer's operating system) to intercept and divert function calls and other data. SSL's interpretation wholly ignoring the use of a shim and construing "intercepting" as "receiving…" was properly rejected. Third, the court correctly followed the logical order of the claimed method steps to hold that certain steps must be carried out in a required order. Because the court's constructions were correct and SSL does not dispute that the jury, as instructed, reached a verdict supported by substantial evidence, the verdict should be affirmed.

Even if the court erred in one of its constructions, SSL is wrong that any such error requires a new trial. SSL has the burden of demonstrating the error was prejudicial and could have led to a different *verdict*, based on the evidence as a whole at trial. Here, affirming the court's construction of either "destination address" or "intercepting" would be enough to sustain the verdict for all three GoTo services, irrespective of any error in the construction of another term.

For the '011 patent, Citrix's cross-appeal addresses three key points entitling it to judgment as a matter of law ("JMOL") on the questions of infringement, invalidity, and willfulness. The accused Access Gateway ("AG") and Netscaler products do not "encrypt files" as the '011 patent claims; the '011 claims were obvious in light of the prior art; and Citrix could not have infringed willfully because its defenses were reasonable and, during the relevant time period, no one

at Citrix knew of the '011 patent or had any reason to believe AG and Netscaler could infringe it. If necessary, Citrix is also entitled to a new trial based on the district court's erroneous exclusion of certain exculpatory evidence relevant to willfulness and its improper admission of irrelevant expert testimony on damages. Finally, the court erred by awarding SSL prejudgment interest for a 4.5 year period during which SSL inexcusably delayed asserting its '011 claims against Citrix.

STATEMENT OF THE ISSUES

'796 Patent

A. Whether to affirm the jury's verdict that Citrix's GoTo services did not infringe Claim 27 when:

1. The court's construction of the term "destination address" to mean a "network address of a computer or server" was correct in light of claim language requiring "transmitting data" over an "open network" and further requiring transmitting files "directly to the destination address"; and the evidence showed the accused ID numbers in the GoTo services were not "destination addresses" under either the court's construction or any construction of "destination address" properly based in the intrinsic evidence;

2. The court's construction of "intercepting" was required by statements in the '796 patent that "the invention" is use of a software shim to intercept and divert both "function calls or requests for service sent by an applications program to a

lower layer set of communications drivers" and "a destination address" of the second client computer; and the software in the accused GoTos did not "intercept" either function calls/requests or destination addresses under either the court's construction or any construction "intercepting" properly based in the intrinsic evidence;

3. The court correctly found the claim language and the specification required the steps of claim 27 to be performed in a logical group order; and the evidence confirmed GoToMyPC and GoToAssist did not perform the steps in the required order; and

4. Each ground for non-infringement is independently supported by substantial evidence, such that any alleged error in instructing the jury on one of those grounds would not have changed the verdict of non-infringement.

B. Whether the district court erred in not naming SSL the "prevailing party" or awarding costs when Citrix prevailed on the primary patent at issue and avoided the substantial majority of SSL's alleged damages.

'011 Patent

A. Whether Citrix is entitled to JMOL of non-infringement where the '011 patent requires an accused product to "encrypt[] files," and SSL did not even address the "encrypt files" limitation, while Citrix's evidence showed Citrix's AG and Netscaler did not "encrypt files";

B. Whether Citrix is entitled to JMOL of obviousness, where two prior art references disclosed the limitations of the '011 claims, and SSL's assertion that two elements were missing was purely conclusory and is contradicted by the references themselves;

C. Whether Citrix was entitled to JMOL or a new trial on willfulness where:

1. Citrix's defenses were objectively reasonable under *Seagate* and *Bard*;

2. SSL failed to show that anyone at Citrix knew about the '011 patent between the time Citrix acquired the accused products and the time SSL amended its complaint in May 2009 to assert the '011 claims; and

3. The court precluded Citrix from introducing evidence of its good faith belief in its defenses, including (i) testimony that Citrix's lead technical executive for AG and Netscaler formed a good faith belief the products did not infringe the '011 patent, and (ii) evidence that Citrix filed for reexamination of the '011 claims and at the time of trial the PTO had *rejected* the patent as obvious based on the same art Citrix relied upon at trial.

D. Whether Citrix was entitled to a new trial on damages when SSL's damages opinion was improperly based on non-comparable, non-patent distribution agreements that were not patent licenses.

E. Whether the court erred by awarding SSL prejudgment interest for the 4.5 year period during which SSL delayed asserting the '011 patent without giving Citrix any notice of its infringement allegations.

STATEMENT OF THE CASE

SSL sued Citrix in April 2008 without prior notice of infringement, alleging the GoTos infringed claim 27 of the '796 patent. Claim 27 recites a method for establishing secure communications between two client computers over an "open network." The GoTos operate in different ways to enable subscribers to access or share data with a remote computer over the Internet, for purposes such as working from home ("GoToMyPC"), giving remote "help desk" assistance ("GoToAssist"), or holding meetings on line ("GoToMeeting").

More than a year into the case, again without prior notice, SSL amended its complaint to add the '011 patent and accuse two different Citrix products, AG and Netscaler, of infringing claims 2, 4 and 7. These products – treated the same for purposes of infringement – enable a computer to communicate securely with a remote server. They were developed independently by third parties and acquired by Citrix in late 2004 and 2005. A1587-1588.

In response to SSL's '011 claims, in 2010 Citrix filed and the PTO granted a request for *ex parte* reexamination. Among the prior art references cited in the reexamination were two references – Takahashi and RFC1508 – that were

ultimately the subject of testimony at trial. A2163-2186. Well before the June 2012 trial, the PTO issued a series of rejections of the claims. A6483-6497; A6540-6557; A6573-6582.

In May 2011, the court (then Hon. T. John Ward) held a *Markman* hearing and later issued a detailed 46-page ruling. A1-46. The court's constructions of three terms in the '796 patent and one term in the '011 patent are relevant to this appeal. Based on the claim language and statements in the specification defining "the invention," the court held that to infringe claim 27 software within one computer called a "shim" must "intercept and divert" certain commands or data (one of which is a "destination address"), and the accused product must perform certain steps of the claimed method in a particular group order. A "shim" is software added between two existing layers to perform a particular function. A110.

For the '011 patent, the court found the accused products must, *inter alia*, use a session key to "encrypt file[s]," and encrypting "files" is different from encrypting data "packets." A32-33.

Judge Ward retired in late 2011 and the case was assigned to newly appointed Hon. J. Rodney Gilstrap. Citrix believed its defenses were strong and moved for summary judgment of non-infringement of both patents, and obviousness of the '011 patent based on Takahashi and RFC1508. SSL opposed

the motions, but did not cross-move. Judge Gilstrap denied Citrix's motions, finding "genuine and disputed issues of material fact as regards to both the non-infringement and invalidity issues." A7294.

In pretrial rulings, the court gave each side 13 hours to present evidence. The court also precluded Citrix from presenting evidence Citrix believed in good faith AG and Netscaler did not infringe the '011 claims and the '011 claims were invalid, based in part on the reexamination record. A6003; A6022.

The amounts at stake for the two patents were vastly different: for the '796 patent, SSL sought past damages of $53m and a 3% royalty for the life of the patent. A1492; A1571. For the '011 patent, SSL sought a lump sum of $10m.

Not surprisingly, the trial focused on the '796 patent. Citrix's expert Dr. Smith testified the GoTos did not infringe for three reasons: (i) the different ID numbers SSL accused of being the claimed "destination address" for each GoTo service were not "destination addresses" because, *inter alia*, they were not addresses and could not be used to address communications between the accused computers; (ii) none of the GoTos "intercepted" function calls/requests for service or destination addresses, and the software modules accused by SSL of doing the intercepting were not "shims"; and (iii) for GoToMyPC and GoToAssist, the method steps were not performed in the required group order.

SSL devoted little trial time to the '011 patent. SSL's expert Dr. Kelly testified in such summary fashion he failed even to mention the "encrypt files" limitation and thus SSL presented no evidence showing this limitation was satisfied. Although Citrix did not have the burden of proof, its witnesses then explained, without rebuttal, that AG and Netscaler did not satisfy the "encrypt files" limitation. *See infra* at 58-61.

Citrix's expert Dr. Smith also testified the claims were invalid as obvious based on Takahashi and RFC1508. SSL's brief rebuttal consisted of Dr. Kelly's disagreement with whether two limitations were disclosed in the art. *See infra* at 61-66.

As to willfulness, SSL never identified anyone at Citrix involved with AG and Netscaler who was aware of the '011 patent before SSL amended its complaint to assert that patent in May 2009. The one person SSL identified as "knowing of" the '011 patent had actually left Citrix two years before Citrix acquired or began selling AG and Netscaler. A1742.

At the close of evidence, the court denied Citrix's JMOL motions. The court allowed willfulness to go to the jury, stating without explanation that "Citrix['s] alleged defenses related to invalidity and infringement are not reasonable as that standard is outlined in the *Bard* case." A2412-2413.

The jury found each of the GoTos did not infringe the '796 patent. A47-48. The verdict form addressed each of the three GoTos separately.

For the '011, the jury found Citrix had willfully infringed, the patent was valid, and SSL was entitled to $10m in lump-sum damages. Given the split verdict, the court decided there was no "prevailing party" and awarded no costs. A62-63. The court enhanced the damages by $5 million for willfulness and awarded prejudgment interest that included the 4.5 years SSL delayed between when Citrix acquired AG and Netscaler and when SSL first asserted the '011 patent in its amended complaint. The court also denied Citrix's renewed JMOL motions and motion for a new trial. A66-100.

STATEMENT OF FACTS

A. "The Invention" Of The '796 Patent Requires Using A Shim To Intercept And Divert A Destination Address And Function Calls/Requests For Service

Claim 27 is a method of "carrying out communications over a multi-tier virtual private network" (VPN) that includes "a server and a plurality of client computers," each with means for transmitting and receiving data on "an open network." A118(20:50-22:5). A VPN is "a system for securing communications between computers over an open network such as the Internet." A109(1:13-15). For purposes of this appeal, the key steps of Claim 27 are:

"***intercepting function calls and requests for service*** sent by an applications program in one of said client computers to a lower level set of communications drivers";

"***intercepting a destination address*** during initialization of communications between said one of said client computers and a second of said client computers on said virtual private network"; and

"transmitting the encrypted files directly ***to the destination address***."

The specification (shared by both patents-in-suit), first depicts the prior art in Figure 2 and then depicts embodiments of the invention in Figures 3-6. A112(8:33-34). Figure 2 shows the operating system ("OS") of a first client computer. The OS is software arranged in levels or layers, together referred to as a "stack." *See* Glossary.

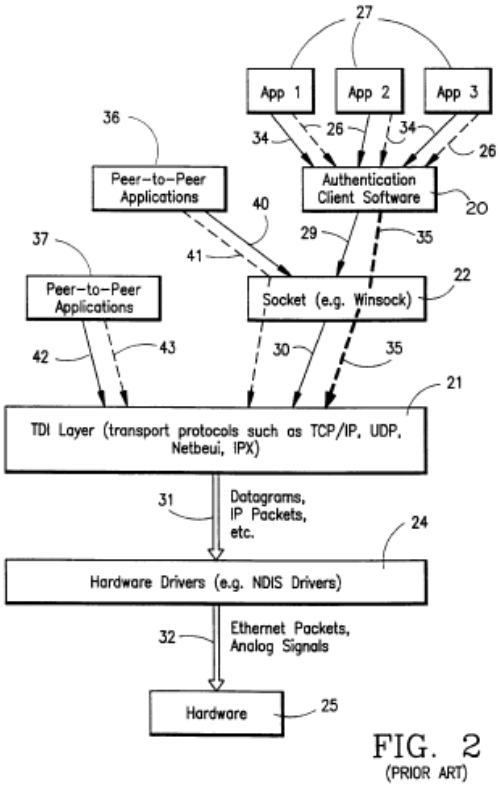


FIG. 2
(PRIOR ART)

At 2:45-3:2, the '796 patent defines the "three basic layers" (from upper to lower) that are "essential to an understanding of the invention": the ***applications level***, the ***transport driver interface ("TDI")*** layer **21**, and the ***network driver interface ("NDI")*** layer **24**. The last two levels are referred to in Claim 27 as the "lower level set of communications drivers." A118.

The "applications level" is the highest logical level, above the TDI layer and NDIS layers, and also is designed to utilize a socket **22** (e.g., Winsock), which serves as an interface between the applications and the TDI layer. A110(3:42-53); A112(8:33-42). The layers operate as described at A110(3:3-53). All three layers in the OS are involved in carrying out communications between an application on a first client computer and an application on a separate server or second client computer.

In the prior art as shown in Figure 2, when a peer-to-peer application **36** wants to send a message to another application on a second client computer, it sends a function call or request for service – *e.g.*, a "connect" instruction, which includes the destination address of the second client computer – to Winsock. Winsock receives the function call and passes it to the TDI layer, which in turn passes it to the NDI layer, through the "hardware **25,**" for transmission over the open network to the destination address of the second client computer. A109-110(2:62-3:2); A112(8:61-67). In networks like the Internet, the message is

contained in formatted data "packets," with a header that includes the destination address. A110(3:16-28).

Figure 2's first client computer also contains applications level "authentication client software **20.**" When called by application **27**, the software **20** uses Winsock to initiate connections to a server, not shown in Figure 2, but also connected to the open network. A112(8:43-50). The computer and server authenticate the parties to the communication, and generate a session key that is used to encrypt data. A111(6:43-48); A113(9:1-10). The software **20** uses the key to encrypt files sent by the applications **27** over the open network. A112(8:56-61). Through this process, applications of type **27** use the software **20** directly to establish a VPN to communicate between client computers ***without*** using the invention.

The patent identifies, as the problem to be solved, that peer-to-peer applications programs **36** and **37**, are ***not*** designed to use the software **20**, or communicate with an outside server to establish a VPN, the way applications **27** can. A113(9:10-25). Rather, applications **36** and **37** must use a different technique, as described in A109(1:26-62 & Figs. 1A-1B).

In the Background of the Invention, the patent states that "the invention" obtains the benefit of both approaches, by adding "shims" to the prior art operating system shown in Figure 2:

> "In order to completely integrate the two approaches and maximize the advantage of each approach, ***the invention*** maintains the applications level infrastructure of prior client server private networking arrangements, ***while adding shims to lower levels*** in order to accommodate a variety of peer-to-peer communications applications …."

A109(1:62-2:20) (emphasis added). A "shim" is "software that is added between two existing layers, which utilizes the same function calls of the existing layers," to the existing layers do not need to be modified. A42; A110(3:60-65).

In the Summary of the Invention, the patent reiterates "the invention" requires use of a shim:

> "These objectives of *the invention* are accomplished by providing a virtual private network for communicating between a server and clients over an open network and in which the clients are equipped with an applications level encryption and mutual authentication program ***which includes at least one shim positioned above either the socket, transport driver interface, or network interface layers of a client computers communicaions hierarchy, and which intercepts function calls or data packets*** …"

A111(6:35-44) (emphasis added). And again at 8:29-32, "the invention" is defined in the Detailed Description of the Preferred Embodiments:

> ***"The invention is not merely the addition of shims to the client software, but involves the manner in which the shims are used*** in the establishment of the authentications and key generation links to the server."

Thus, as the district court found, the patent defines "the invention" and distinguishes it from the prior art based on the addition of software "shims" that are used to intercept function calls and divert those calls to the security software **20**

to force the peer-to-peer applications to use that software when they attempt to open a connection over an open network. A23-27. Every embodiment uses shims to intercept function calls/requests and a destination address. A104-106(Figs. 3-5); A111-112(6:35-48; 7:15-24; 8:29-32); A113(10:66-11:7 (describing Figs 3-6)); A114(11:59-60 (Fig. 7)). No other method for performing the "intercepting" steps, besides use of a shim, is described in the patent.

Figure 3 shows a preferred embodiment of the invention, in which "the arrangement of Fig. 2" is modified "by adding a socket shim **50**" (in red) to the prior art architecture of Figure 2:

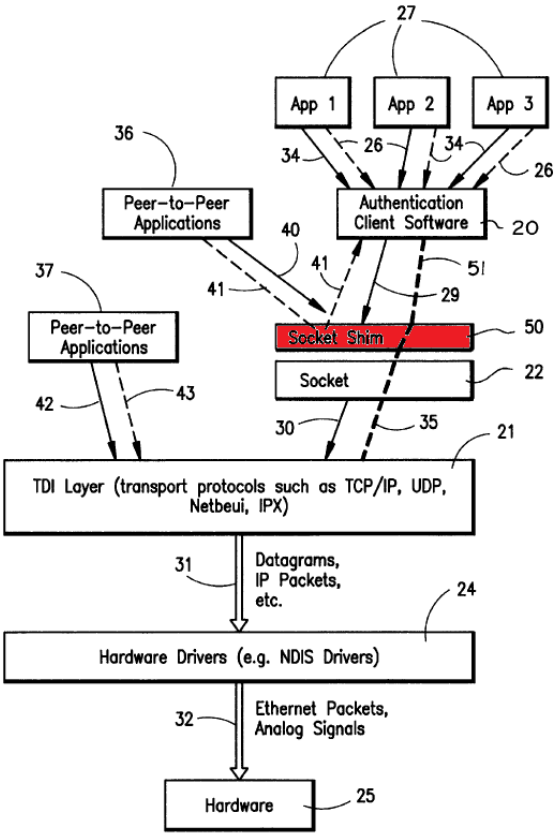


FIG. 3

The socket shim **50,** "operates by hooking or intercepting call initiation function calls **40** made to the socket" and "in response thereto, having the authentication client software [**20]** initiate communications with" the remote server **23** (not shown). A113(9:47-53). The shim **50** also intercepts the destination address of the remote client computer and supplies it to the authentication client software, which in turn provides it to the server. A113(9:60-10:11). Figures 3-5 exemplify different locations in a network stack where the shim can be placed. A104-106.

Using Figures 6-7, the patent further explains the steps of Claim 27 and the order in which they are performed, as reflected in the court's claim construction. Figure 6 shows a VPN with a server and two client computers (peers) communicating over the open network. A107. An application on Computer A opens a link with Computer B by making function calls/requests to "a lower level set of communications drivers." A114. Before the function call reaches the intended lower level drivers, it is intercepted and diverted by a shim on Computer A. A111-114(6:35-59; 6:66-7:6; 8:23-32; 9:42-49; 10:66-11:14); A103-106(Figs. 2-5). The interception causes "an applications level authentication and encryption program" in Computer A to communicate with the server in order to generate a session key. A118-119[1]; A113(9:42-59); A114(11:23-37).

[1] Claim 27 erroneously claims some of these steps twice.

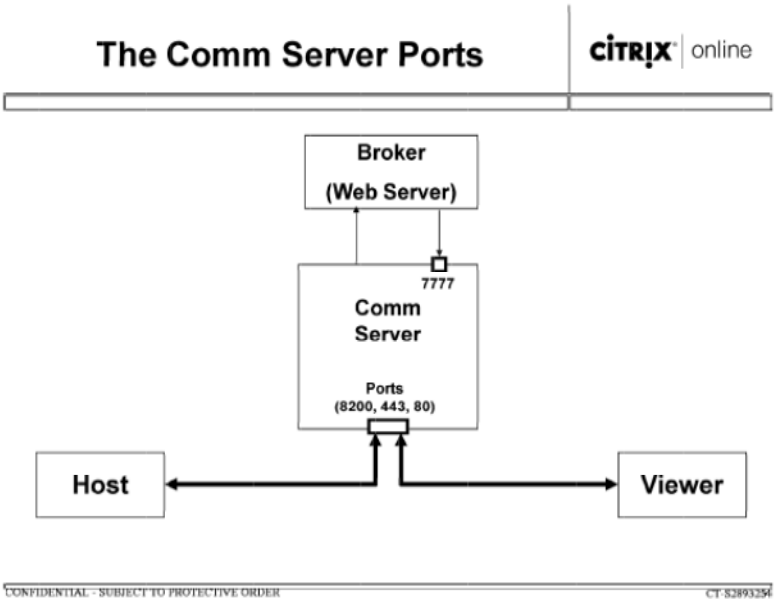
Computer B needs the same session key as Computer A to decrypt the encrypted files sent by Computer A. Accordingly, Computer A's shim also intercepts and diverts the destination address of Computer B to the authentication client software **20**. A2957. Computer A subsequently transmits this address to the Server, A113(9:62-67), to enable the Server to open a communication link with Computer B. A2957(27[G]); *see also* A113(9:60-10:8). The Server enables Computer B to "recreate" the key generated earlier. A2957; *see also* A114(11:24-37). Computer A uses the key to encrypt files, and the encrypted files are transmitted directly to the destination address of Computer B on the open network. A2957.

B. Citrix's GoTo Services Do Not Practice Three Key Limitations Of The '796 Patent

Citrix's three GoTo services were originally developed by another company and then acquired by Citrix in March 2004. A1703-1704; A1823. Each of the GoTos operates differently, but each enables a GoTo subscriber at a remote computer to use Citrix's centralized servers to help set up a secure communication to one or more other computers. The Citrix GoTo software is designed so ***all*** relevant communications from the subscriber's computer are sent to a Citrix server to set up and carry out the secure communications; and as a result no "intercepting" of any function calls/requests or destination addresses is ever required. A2054-2065. And in the GoTos, the remote computers ("endpoint

computers") and servers communicate only over the Internet, using IP packets. A1440-1441. The endpoint computers do not know the destination address of the other endpoint computer they are communicating with, and do not address data packets to that address. A1441.

GoToMyPC: GoToMyPC allows subscribers to, *e.g.*, use a home computer to access their office computer over the Internet. A1825. The GoTo endpoint computers only communicate with each other *indirectly*, using a central Citrix server called the CommServer. A1862-1868; A1887; A2117. The user's endpoint computer is called the "Viewer," and the endpoint computer to be remotely accessed (*e.g.*, office computer) is the "Host." A1881.



A4459. SSL accused the Viewer as the first client computer and the Host as the second client computer. A1253-1255.

A user at the Viewer can access GoToMyPC by opening a web browser and logging into GoToMyPC's website, located on another Citrix server, the Broker. A1881. The Broker has a list of computers the user can access remotely, each with an assigned ID number called a MachineNameKey (a/k/a QuickConnectID). A1885.

SSL accused the MachineNameKey as being the "destination address" referred to in the claims. But the MachineNameKey is *not* an address at all; it is an internal identification number. A2124-2125. It was undisputed that the MachineNameKey cannot be used to "address" any message or data that can be sent by the Viewer. A2124-2125; A1419-1422. Therefore, the MachineNameKey could not satisfy the claim limitation of "transmitting encrypted files directly to the destination address." A2123-2128.

The MachineNameKey also is not "intercepted" within the Viewer, as Claim 27 requires. A1885-1886. To the contrary, the ***Broker*** originally supplies the MachineNameKey ***to*** the Viewer. A1885-1886. When the user selects a particular computer to be accessed remotely, the Citrix software is designed to return the MachineNameKey to the Broker. A1885-1886. Within the Viewer computer, the MachineNameKey is passed down the stack of the operating system and is sent back to the Broker, precisely as intended. A1885-1887.

Furthermore, the Viewer computer has no "shim," let alone one that "intercept[s]" function calls/requests or a destination address. A2049-2062. Citrix's application software includes a "CommStack" used for communications between an endpoint and the CommServer. A1873-1875; A7014-7044. The CommStack sends data to the "Winsock" portion of the Microsoft OS (A1875-1877; A2052-2053), and from there the data proceeds down the rest of the OS stack, and then out over the Internet. SSL accused two things of being a "shim" for purposes of the "intercepting" steps: (i) the "lower layers of the CommStack" and (ii) Winsock. A1294; A1301-1302. However, neither the CommStack nor Winsock is a "shim," and neither "intercepts" anything. Rather, they pass the function calls/requests made by the Citrix software down through the stack to the lower level drivers where they are processed as intended. A2054--2059.

Finally, GoToMyPC does not perform the claimed steps in the order required by the court's claim construction. A2129-2135. For example, in GoToMyPC, the session key is not generated until ***after*** the server contacts the second client computer, while the claim requires the key to be generated *before* the second computer is contacted. A2131-2132; A15.

GoToAssist: GoToAssist enables an "expert" to access a customer's computer over the Internet to provide "help desk"-type services. Its system architecture is similar to that of GoToMyPC. A1894. SSL accused the expert's

and customer's computers as the first and second client computers, respectively. GoToAssist starts with the customer contacting the Broker server to post a help request. A1894-1895. The Broker assigns a SessionID (aka Query Key) to the request. A1895. Thereafter, when the expert contacts the Broker, the Broker provides the expert's computer a list of help requests, each with its pre-assigned SessionID. A1895. SSL accused the SessionID as being the "destination address."

The SessionID, however, is not an "address," nor does it even identify any computer or any "destination." Rather, it merely identifies a help request. A2121-2123. Further, no files can be "transmit[ed] … directly to" the SessionID, as the claim requires. A1895-1896; A1903. And, the SessionID is not used in communications between the customer and expert endpoints. A1901; A1907.

Nor is the SessionID ever "intercepted." When the expert "accepts" the help request, the Citrix software is designed to send a response that includes the SessionID back to the Broker. A1897. As with GoToMyPC, the SessionID, and all function calls/requests, are processed and passed down the stack – including through the CommStack and Winsock – precisely as intended. A2056-2062.

Finally, GoToAssist does not perform the claimed steps in the order required by the Court's claim construction, for several reasons, depending on the specific version of GoToAssist. A2136-2150.

GoToMeeting: GoToMeeting allows a subscriber to set up on-line meetings from her own computer. Multiple users can "meet" over the Internet and view a single presentation from different locations. One subscriber is the "Organizer," all other attendees are "participants." A1825-1826. SSL accused the Organizer's computer as the first client computer and participants' computers as the second client computer(s). A1288-1290; A1305.

In GoToMeeting, the Organizer contacts the Broker to set a time and date for the meeting. The Broker assigns a "MeetingID" for the meeting. A1863-1864. The Organizer then contacts the possible meeting participants by separate means (*e.g.*, email), and gives them all the same the MeetingID, a call-in number, and an access link over the Internet. A1864. The Organizer and the participants join the meeting by calling and logging in, using the MeetingID as a "ticket" to the meeting. A1864-1865. SSL accused the MeetingID as being a "destination address."

The MeetingID, however, is not an "address," and files cannot be transmitted "directly to" a MeetingID. A2110. Indeed, every attendee to a meeting has the exact same MeetingID, so the MeetingID does not even distinguish one participant's computer from another. A2117. The MeetingID thus is not even indicative of a "destination" to which data is being sent. A2114-2117. Rather, it merely identifies a particular meeting that can be accessed by multiple

computers, each of which have their own network addresses and communicate through separate connections with the CommServer. A2114-2117.

Further, as with the other GoTos, neither the CommStack nor Winsock "intercepts" any function calls/requests or the MeetingID. A2060-2062. For GoToMeeting, Citrix did not argue the "step order" issue at trial.

C. The '011 Patent Requires "Encrypt[ing] *Files*," Not Packets

Claims 2, 4 and 7 of the '011 patent cover a network, software and method for establishing secure links between a client computer and a server over an open network. Like the '796 claim, each claim requires intercepting function calls/requests sent by an applications program to a lower level set of communications drivers. The interception causes an applications level authentication and encryption program in the client computer to communicate with the server and generate a session key. A134. Such limitations were not in dispute for AG and Netscaler.

There was a dispute, however, as to the limitation in each claim requiring the key to be used to "encrypt files." A134. As the court explained, the patent's use of the word "files" makes clear "the encryption must occur at the file level." A32. As the court put it: "[T]he claim language distinguishes encrypting files from encrypting packets," and "[t]he patents state that datagrams or packets *carry* encrypted files." A31. Thus, "the term [files] cannot be construed so broadly that

it would include 'packets'…." A32. It construed "encrypt files" to mean "to render a set of data used by a program unintelligible without decrypting." A33. SSL therefore had to prove AG and Netscaler did not encrypt packets or even data generally, but specifically encrypted "***files***."

D. AG And Netscaler Do Not "Encrypt Files"

As explained further below, SSL provided no evidence concerning the "encrypt files" limitation. SSL's expert Dr. Kelly never discussed or mentioned that limitation or provided any evidence AG or Netscaler "encrypt files." *See infra* at 58-61; A1355-1377.

Citrix's technician Mr. Murgia then testified that AG and Netscaler do not "encrypt files," but rather encrypt data at the packet level, and Dr. Smith opined that the products do not infringe under the Court's construction. A1942; A2189-2190. SSL never rebutted this evidence.

E. The Combination Of Takahashi And RFC1508 Rendered The '011 Claims Obvious

At trial, Dr. Smith also explained why the combination of Takahashi and RFC1508 disclosed all the claim limitations and rendered the '011 claims obvious, A2166-2186, including authentication and encryption software at the "applications level," A2171; A6866(Fig. 2), and mutual authentication of the client and server, A2180, A06875-76 (discussing authentication by use of tokens), A2180. *See infra* at 61-66.

In rebuttal, Dr. Kelly made only two points in highly conclusory testimony: (i) he "disagreed" that Takahashi's authentication and encryption software was at the "applications level," and (ii) he opined that RFC1508 "does not show you how to do authentication," A2368-2372.

F. SSL Did Not Prove Anyone At Citrix Involved With AG And Netscaler Knew Of The '011 Patent

With respect to willfulness, SSL accused Citrix of willful infringement solely on the ground that Citrix "knew of the patents" as a result of a pre-lawsuit business relationship between Citrix and V-One, the original assignee of the patents. SSL Br. 22. However, a chronology shows Citrix's relationship with V-One had ended and the Citrix employee who "had knowledge" left Citrix more than two years before Citrix acquired the AG and Netscaler products in late 2004 and 2005. SSL did not assert the '011 patent until amending its complaint in 2009, and SSL did not identify any Citrix person involved with AG and Netscaler who had any knowledge of the '011 patent before that amendment.

2000-2001: Citrix and V-One enter into "License and Distribution Agreements" for Citrix to distribute V-One's "SmartGate" software, rebranded as a Citrix product. An appendix to the agreements called a "certificate of originality," listed several V-One patents and pending applications, including the '011 patent, but it was undisputed V-One did not license *any* patent rights to Citrix. A1110, A1145-1146; A4843-4957. Citrix's project manager working with V-One at the

time, Bill Mangum, acknowledged he knew of the '011 patent. He testified, however, that he could not recall ever seeing it, reading it or discussing it with anyone at Citrix. A1750-1751.

April 2002: Mr. Mangum leaves Citrix before Citrix ends its relationship with V-One. A1742; A1763.

Fall 2003: V-One notifies other companies, but not Citrix, of the existence and scope of the '011 and other patents, in hopes of obtaining licensing revenues. A6990-7013.

Late 2004-2005: Citrix acquires and begins selling AG and Netscaler in December 2004 and August 2005, respectively. A1587-1588; A1701; A1588; A1714-1715. SSL acquires the '011 patent from V-One in June 2005. A1195.

May 2009: Four-and-a-half years later, without any prior notice, SSL adds the '011 patent to this case by amendment. A6755-6766.

Once SSL amended its complaint to add the '011 patent, Citrix investigated the patent, determined in good faith that it did not infringe and the patent was invalid, and thereafter filed for reexamination of the '011 patent. However, the district court prevented Mr. Murgia, Citrix's Chief Software Architect, from testifying that he reviewed the '011 claims and formed a good faith belief that AG and Netscaler did not infringe the patents. A1668-1672. The court also excluded

any evidence concerning Citrix's filing of the '011 reexamination and the results of the reexamination. A2079-2080.

G. SSL's Damages Evidence Relied On Non-Comparable, Non-Patent Distribution Agreements

As damages for the '011 patent, the jury awarded a lump sum payment of $10m, adopting the opinion of SSL's expert, Mr. Reed. Over Citrix's objections, Mr. Reed based his royalty rate on the essentially identical 2000 and 2001 "License and Distribution Agreement" agreements between Citrix and V-One. A1609-1610.

It was undisputed, however, that these agreements were not patent licenses, but instead gave Citrix merely a right to distribute V-One's Smartgate software and other benefits that would not be contained in a patent license. A1609-1614. Moreover, SSL specifically denied that Smartgate even practiced the '011 claims. A7295.

SUMMARY OF ARGUMENT

'796 Patent:

The district court correctly construed ***"destination address"*** as the "network address of a computer or server." SSL challenges the word "network." But Claim 27 requires communications over an "*open network*," encrypting files "before transmittal *over said open network*" and transmitting those files "directly to a *destination address*." A "network" address fits this language precisely. In

contrast, SSL's construction – "identifier for a desired location" – would improperly read the word "address" out of the claim.

Moreover, the evidence is overwhelming that the accused ID numbers – the MeetingID, SessionID and MachineNameKey – are not "addresses" in any sense. Thus, even if the court's construction is found erroneous, no reasonable juror would find these ID numbers to be "destination addresses" based on any construction consistent with the intrinsic evidence.

The court also correctly construed ***"intercepting"*** based on the specification's repeated statements defining "the invention" as use of a shim to intercept and divert function calls/requests and a destination address. SSL's construction of "intercepting" as merely "receiving from a software module that which concerns another software module" is inconsistent with the plain meaning of "intercepting." Further refuting the notion that "intercepting" is merely receiving, the intrinsic evidence teaches how data sent from an application to lower levels of the OS routinely passes through intermediate software without being "intercepted."

Even if the court erred in construing "intercepting," any such error would be harmless because SSL still could not prove under any construction of "intercepting" consistent with the intrinsic evidence that the software in the accused first client computers "intercepts" function calls/requests or a destination address. In the GoTos, function calls/requests are sent from the application

software to Winsock and from Winsock to the lower levels for processing and ultimate delivery to the intended destination, without "interception" of any kind.

The court's ***step order grouping*** correctly follows the logical flow of the claim language and the specification. SSL alleges only two errors in the court's step order grouping, but in each instance the construction is directly supported by the claim language and the specification, and substantial evidence supports the conclusion that the step order was not met in GoToMyPC and GoToAssist.

SSL contends that this Court should remand if any one of the court's claim constructions is incorrect. When this Court "determine[s] on appeal, as a matter of law, that a trial judge has misinterpreted a patent claim, we independently construe the claim to determine its correct meaning, and then determine if the facts presented at trial can support the appealed judgment." *Exxon Chem. Patents v. Lubrizol,* 64 F.3d 1553, 1560 (Fed. Cir. 1995). Here, there are three independent claim construction issues, each supported by substantial trial evidence. SSL does not even attempt to meet its burden of showing ***the verdict*** would have been different for each of the GoTo products if it convinces the Court of only one proposed construction, or if a corrected construction is different from the obviously incorrect constructions posed by SSL.

Finally, the court did not err in declining to name SSL the "prevailing party" or award costs, given Citrix's victory on the principal patent at issue.

‘011 Patent:

Because SSL chose to present its infringement case summarily, it did not introduce any evidence that AG and Netscaler “encrypt ***files***.” Citrix’s Mr. Murgia and Dr. Smith testified that the products did not “encrypt files,” and thus did not infringe. With no evidence supporting a verdict on “encrypt files,” JMOL should have been entered for Citrix.

All three ‘011 claims are obvious based on the combination of Takahashi and RFC1508, based on the references and Dr. Smith’s testimony. Dr. Kelly’s conclusory testimony that two elements are missing should be disregarded. He did not explain his conclusion, and his opinion is contradicted both by the references and by statements in the patent defining “applications level” software.

With respect to willfulness, as a matter of law, Citrix’s non-infringement and invalidity defenses were objectively reasonable and Citrix did not act recklessly, particularly in light of the repeated rejections of the ‘011 claims during reexamination. As to the subjective prong of willfulness, SSL provided no evidence that anyone at Citrix had involved with AG or Netscaler had knowledge of the patent or had any reason to believe Citrix might infringe before SSL amended its complaint to add the ‘011 patent.

If the Court does not reverse the judgment, it should remand for (i) a new trial on willfulness because the Court erred by precluding Citrix’s witnesses from

testifying to Citrix's good faith belief that the accused products did not infringe the '011 patent, and to the results of the pending reexamination as supporting Citrix's view the '011 was invalid, and/or (ii) a new trial on damages because the court erred in allowing SSL's damages expert to base his opinion on License and Distribution Agreements that were not patent licenses, but only constituted Citrix's agreement to distribute a product that SSL denied embodied the patents.

Finally, the Court erred in granting prejudgment interest for the 4.5 years during which SSL inexcusably delayed amending its complaint to assert its ' 011 claims.

STANDARDS OF REVIEW

The court's claim construction is reviewed *de novo*. *Cybor v. FAS Techs.*, 138 F.3d 1448, 1456 (Fed. Cir. 1998). This standard may be modified in *Lighting Ballast Control v. Philips Elec. North America*, Nos. 2012-1014, -1015 (Fed. Cir.) (rehearing *en banc* pending).

If a jury instruction based on the claim construction was erroneous, SSL cannot win reversal "if substantial evidence appears in the record supporting the jury's verdict and if correction of the errors in a jury instruction on claim construction would not have changed the result, given the evidence present." *Teleflex v. Ficosa N.A.*, 299 F.3d 1313, 1328 (Fed. Cir. 2002).

The denial of JMOL is reviewed "without deference." *Johns Hopkins Univ.*

v. Datascope, 543 F.3d 1342, 1344-45 (Fed. Cir. 2008). JMOL must be granted if the jury's verdict is not supported by substantial evidence. *ClearValue v. Pearl River Polymers,* 668 F.3d 1340, 1343 (Fed. Cir. 2012). Denial of a new-trial motion is reviewed for abuse of discretion. *i4i Ltd. v. Microsoft*, 598 F.3d 831, 841 (Fed. Cir. 2010).

This Court reviews the "jury's conclusions on obviousness, a question of law, without deference, and the underlying findings of fact, whether explicit or implicit within the verdict, for substantial evidence." *John Hopkins,* 543 F.3d at 1345.

Review of the court's determination of the "objective prong" of the willfulness standard is *de novo*. *Bard Peripheral Vascular, Inc. v. W.L. Gore,* 682 F.3d 1003, 1007 (Fed. Cir. 2012). Review of the "subjective prong" is for substantial evidence. *Id.* at 1008.

A court's decision to exclude evidence is reviewed for abuse of discretion. *Lucent Techs. v. Gateway*, 580 F.3d 1301, 1329 (Fed. Cir. 2009).

A decision not to award costs and an award of prejudgment interest is reviewed for abuse of discretion. *Energy Transp. Group v. William Demant Holding*, 697 F.3d 1342, 1358 (Fed. Cir. 2012).

ARGUMENT

I. THE JURY'S VERDICT THAT CITRIX'S GOTOS DID NOT INFRINGE THE '796 PATENT SHOULD BE AFFIRMED

Citrix's evidence at trial fully supported three independent grounds for non-infringement: the accused ID numbers used by the GoTos were not "destination addresses;" the GoTos did not "intercept" a destination address or function calls/requests; and GoToMyPC and GoToAssist did not meet the step order requirements. On appeal, SSL never argues that, if the court's claim constructions were correct, Citrix failed to adduce substantial evidence to support the jury's non-infringement verdict. As shown below, for each of the challenged grounds, ***the court's construction was correct***, SSL's alternative constructions were demonstrably inconsistent with the claim language and the specification, and Citrix adduced substantial evidence to support the verdict.

Even if this Court disagrees with one or more of the court's constructions, it still must affirm "if correction of the errors in a jury instruction on claim construction would not have changed the result, given the evidence presented." *Teleflex,* 299 F.3d at 1328. Here, the evidence is such that the GoTos would not infringe under the district court's construction – or any construction consistent with the intrinsic evidence – of "destination address" or "intercepting," and GoToMyPC and GoToAssist simply do not infringe under the step order

limitation. SSL cannot meet its burden of proving any alleged error was actually prejudicial.

A. "Destination Address"

1. In a Claim Concerning Communications Between Computers on an "Open Network," the Court Correctly Construed "Destination Address" to be a "Network Address"

The district court correctly construed "destination address" as "the network address of a computer or server." A33-35. SSL challenges inclusion of "network," but the claim language confirms a destination address is a "network address." Claim 27 is a "method of carrying out communications over a multi-tier [VPN]" in which computers and servers "transmit[] data to and receiv[e] data from an open network." A118(20:50-55). The patent defines a VPN as a "system for securing communications between computers over an open network such as the Internet." A109(1:14-16). The claim itself also requires encrypting files before they are transmitted "over said open network" and "transmitting the encrypted files directly to the destination address." A118(20:64-65); A119(22:4-5). Thus, the destination is a computer on the network, and the destination address is the network address of that computer.

The specification confirms that "destination address" has its ordinary meaning in this context: a network address. For example, the specification identifies the "destination address" as a part of the address portion of data packets.

A110(3:16-24); A113(10:43-47) ("At [the NDIS] layer, the shim 55 intercepts IP packets from applications 56 … checks the destination address…").

Contrary to SSL's assertion, the court's construction did not mandate a "specific format" of network address. SSL Br. 46. The term "network" is generic, and different computer networks use different data transmission formats and thus different address formats. During *Markman,* the court explicitly stated "the claimed invention is not limited to IP based protocols and may use non-IP based protocols," citing the same specification language SSL now cites. *Compare id. with* A34.

SSL also claims the court's construction improperly allowed Citrix to argue that "destination address" is limited to an IP address. SSL Br. 46-47. The district court did not abuse its discretion in denying SSL's new-trial motion on this ground, A79-80, and in fact Citrix made no such argument. Rather, Dr. Smith informed the jury of the court's construction. A2103-2104. He explained that computers have network addresses so packets can be delivered to them, as houses have street addresses for mail delivery. A2105-2108. Dr. Smith then testified that ***in the GoTos***, the accused computers' network addresses are their IP addresses, because they use an IP-based protocol. He stated, twice, that he was *not* opining "that the destination address must ***always*** be the IP address," and Citrix never made any such assertion. A2233-2234 (emphasis added). Rather, an IP address is

an *example* of a network address. A2226. That was perfectly correct, and even SSL's expert agreed an IP address is a "type of network address." A1271.

2. The Identification Numbers Used by the GoTos are Not "Addresses" and are Not Used to Route Data Between Computers, so the GoTos Would Not Infringe Under Any Construction of "Destination Address" Properly Based on the Intrinsic Evidence

Substantial evidence proves that, under the court's construction, the Citrix MeetingID, SessionID and MachineNameKey are not "destination addresses" to which encrypted files are "transmit[ed] … directly." For one thing, the GoTos use IP addresses, *not* the ID numbers, as the destination address of the accused second client computer. A2113-2114. And there is no direct transmission to the ID numbers: for each of the GoTos, the accused first client computer ***does not know*** the second client computer's IP address, but only knows and transmits data to the address of the CommServer. A2112-2114.

Even if the word "network" is taken out of the court's construction, the GoTos would still not infringe because the ID numbers are not "addresses" at all. For example, the MeetingID in GoToMeeting does not even uniquely identify any computer. It is just a number assigned to an electronic "meeting" that can be attended by many people, each using the same MeetingID to enter the meeting. A2110. The MeetingID says nothing about any one of the client computers being used to participate in the meeting or the address of any one of those computers.

A2115-2116. Each of those computers has its own IP address, which is ***not*** the MeetingID shared by all participants. A2110-2113. Similarly, in GoToAssist, the SessionID is not an address, but is an ID number that identifies a help request, not a computer. A1895-1896. Likewise, in GoToMyPC, the MachineNameKey is an internal ID number, not an "address." A1885. Data cannot be addressed with, or transmitted to the Session ID or the MachineNameKey. A1896; A2127-2128.

Because the GoTo ID numbers are not "addresses," SSL tried to convince the court to construe "destination address" as any "identifier for a desired location." SSL Br. 45. But the court properly rejected SSL's construction because it writes the term "address" out of the claim entirely. A34. "[E]very limitation of a claim is material." *Flex-Rest v. Steelcase*, 455 F.3d 1351, 1361 (Fed. Cir. 2006). While there may be different ways to identify a destination, the patent specifically claims a "destination ***address***," not a "destination" or "identifier for a desired location."

For all the reasons stated, Citrix submits the court's construction of "destination addresses" is correct. But even if this Court disagrees, given the evidence at trial, under any construction of "destination address" that is properly based on the intrinsic evidence, no reasonable juror could have concluded the accused ID numbers are "destination addresses." Accordingly, there is no basis for a remand. *See Bowers v. Baystate Tech.*, 320 F.3d 1317, 1334 (Fed. Cir. 2003)

(affirming a jury verdict despite a change in construction where "the record on appeal supplies substantial evidence to support the jury verdict under the new claim construction."); *Weinar v. Rollform,* 744 F.2d 797, 808 (Fed. Cir. 1984) (reversal "not available" where "the evidence in support of the verdict is so overwhelming that the same verdict would necessarily be reached absent the error"), *cert. denied,* 470 U.S. 1084 (1985).

B. "Intercepting"

1. The Patent's Statements that "The Invention" is Using a Shim to Intercept and Divert Function Calls and Destination Addresses Mandate the Court's Construction of "Intercepting"

The district court also correctly construed the term "intercepting" in the phrases "intercepting a destination address" and "intercepting function calls or requests for service" to require "using a shim to intercept or divert" the address, function calls or requests. A27; A35. As the court stated, "the use of a shim to intercept function calls and requests for services is repeatedly highlighted throughout the patents as the key feature of the claimed invention." A25.

The statements in the patent defining "the invention" confirm the court's conclusion that "using a shim to intercept or divert" the destination address or function calls/requests is required. *Honeywell Int'l v. ITT Indus.*, 452 F.3d 1312, 1318 (Fed. Cir. 2006). The '796 patent states that "***[t]he invention is not merely the addition of shims to the client software, but involves the manner in which the***

shims are used in the establishment of the authentications and key generation links to the server." A112(8:23-32) (emphasis added).

Indeed, the use of shims, according to the patent, is what distinguishes the invention from the two prior art approaches to VPNs. A102-103(Figs. 1A, 1B, 2); A109(1:27-62). "The invention" integrates the prior art approaches by "adding shims to lower levels." A109(2:9-16); *see also* A103-106(Figs. 2-5); A112(8:33-35). The patent describes "shims" as among the "principal components of the overall system." A113(10:66-11:8). And, the patent recites multiple objectives of "the invention," A111(5:66-6:34), then states these objectives are met by using "at least one shim" which "intercepts function calls or data packets." A111(6:35-43). Indeed, the *only* structure described in the patents as "intercepting" function calls or destination addresses is a "shim." No embodiment of the invention that does not use a shim is disclosed.

The patent also emphasizes that the shims are used to intercept ***and*** divert function calls/requests and a destination address. The specification states that function calls/requests are sent by application 36 to the lower layer drivers, but are intercepted by the shim *50* and diverted to the applications layer authentication and encryption program ***20***:

> "The shim 50 operates by ***hooking or intercepting*** call initiation function calls 40 made to the socket and, in response thereto, having the authentication client software initiate communications with the authentication server 23 … Shim 50 also causes files 41 intended for the

> TDI layer to be diverted to the authentication software." A113(9:47-54)(emphasis added).

Other passages also show that intercepting and diverting are synonymous:

> "***Like the socket shim***, implementation of the TDI shim essentially simply involves ***diverting*** certain information to the client software in order to establish a communications link with the authentication server." A113(10:24-28)(emphasis added)

> "In one especially preferred embodiment of the invention, the client software includes ***a Winsock shim arranged to intercept function*** calls to the Winsock library on a client machine ***and redirect*** initial communications through the authentication client software to the authentication server so that any ***function calls to the Winsock library of programs are intercepted by the shim and carried out by the applications level security program***." A111-112(6:66-7-6)(emphasis added).

Indeed, by this interception and diversion, the shim 50 carries out its "principal function," which is "to arrange for the destination [] address of the communication to be supplied to both the authentication client software [20] and to [the remote] authentication server, even though the peer application assumes that it is communicating only with the peer application." A113(9:64-10:2). Thus, the specification expressly teaches that "intercepting" includes "diversion" to the authentication client software, as court ruled.

SSL argues that "[i]t is certainly possible to 'intercept' something without 'diverting' it" (SSL Br. 29), but in fact the ordinary meaning of "intercepting" inherently involves diverting possession, control or use. *See* Definition of intercept, *available at http://www.merriam-webster.com/dictionary/intercept* ("to

stop and take someone or something that is going from one place *to another place* before that person or thing gets there"). In football, an "interception" requires the opposing team to catch the ball and thus divert possession, control and use of the ball away from the passing team. And for ***this*** patent, the heart of "the invention" is using a shim whose "principal function" is to intercept and divert function calls and destination addresses from their intended destination and provide them to the applications level encryption and authentication software. *See* A113(9:64-10:2). The district court correctly recognized that, for *this* patent, intercepting and diverting are one and the same.

This Court should reject SSL's contention that a quote from the Background of the Invention "makes clear that intercepting can be done without a shim." SSL Br. 39-40. The quote states: "The changes made by the present invention to the conventional client server virtual private network may be thought of as, essentially, the addition of means, most conveniently implemented as shims, which add a secured mutual authentication and session key generation channel between the server and all parties to a communication, at all levels at which a communication can be carried out." A109(2:37-44). Contrary to SSL's suggestion, this passage is *not* referring to "intercepting," but even more important, ***everywhere else*** in the patent, the *only* way "the invention" carries out interception is by use of a shim. No other way of doing it is disclosed.

SSL also takes out of context another passage in the Background that does not refer to "the invention" or to "intercepting," but instead discusses different ways the prior art incorporated "encryption and authentication functions" into an existing OS. SSL Br. 39-40 (citing A110(3:60-65)). One way is to modify an existing layer to add the functions. A110(3:54-65). But "[i]f possible, it is generally desirable to minimize modification of the existing levels by adding a layer *to perform the desired functions*…. Such a layer is commonly referred to as a 'shim.'" A110(3:60-64) (emphasis added). The "desired functions" are the "encryption and authenticating functions." There is no reference here to intercepting and diverting, either with or without a shim. Rather, the word "shim" is used to explain that such a layer added between existing levels is called a "shim."

SSL makes a similar error when it cites the Background at A110(4:44-53) as if it describes an alternative embodiment that does not use shims to intercept function calls or destination addresses. SSL Br. 10. However, the cited passage says no such thing. Rather, the patent refers there to already existing, alternative ways to "implement the mutual authentication and encryption services *at the lower layers*." A110(4:28-30). The patent then disparages each of the possible options as "fundamentally different in concept than the present invention," or as requiring

"modifying the TCP/IP stack and or hardware to provide encryption" and "not utilized by the preferred embodiment of the present invention." A110(4:38-52).

Finally, SSL's reference to a passage in the Background stating "client authentication software 20 intercepts interconnect calls from client authentication software supported applications **27**" (SSL Br. 40), also does not support SSL's argument that shims are not required for the "intercepting" steps of the claimed invention. Most important, the passage does not describe an embodiment of the claimed invention, but rather describes prior art architecture found in Figure 2, that does not use the invention. A103; A112(8:33-45). SSL does not identify any embodiment ***of the invention*** that does not use a shim to carry out the claimed "intercepting."

2. Claim Differentiation does Not Override the Statements in the Specification Requiring Interception by a Shim

SSL next asserts that the Court "violated the cardinal claim-differentiation rule" by following the patent's teaching that the invention requires a shim. SSL Br. 35. Preliminarily, there is no "cardinal rule" of claim differentiation: "[c]laim differentiation is a rule of thumb that does not trump the clear import of the specification." *Eon-Net v. Flagstar Bancorp*, 653 F.3d 1314, 1323 (Fed. Cir. 2011). It "cannot alter a definition that is otherwise clear from the claim language, description, and prosecution history." *O.I. v. Tekmar,* 115 F.3d 1576, 1582 (Fed.

Cir. 1997); *see also AstraZeneca AB v. Hanmi USA*, No. 2013-1490, Slip Op. at 10 (Fed. Cir. Dec. 19, 2013).

In addition, dependent claim 28, which SSL relies upon, is differentiated from claim 27 not only by use of the word "shim," but also by adding a limitation on the *location* of the shim that is used for "intercepting a destination address" (*i.e.*, "between a peer-to-peer program and a layer of a communications driver architecture of said one of the two client computers") and by reciting a "peer-to-peer applications program." A24; A118-119. Alternative locations for the shim are shown in Figs. 3-5. A104-106. Even SSL's Dr. Kelly testified that claim 27 contains no "positional requirement" for the shim, stating, "The language doesn't … give you any indication of where the shim needs to be." A1412-1414.

SSL next argues that construing "intercepting" in claim 27 to require a shim renders superfluous the language in claims 2 and 4 of the '011 patent requiring a "shim arranged to intercept." SSL Br. 37. SSL makes this erroneous argument by considering only a *portion* of the claim limitation out of context. The entire limitation includes *what* the shim is arranged to intercept – *i.e.* "a shim arranged to intercept function calls and requests for service…." Here, the district court did not construe either "shim" or "intercepting" to include *what* is intercepted. There is thus nothing superfluous about this claim limitation. Moreover SSL's citation to *Digital-Vending Servs. v. University of Phoenix* is off-point, as it did not involve

explicit statements defining the invention in a way that supported the court's construction at issue. 672 F.3d 1270, 1274 (Fed. Cir. 2012).

Finally, the district court correctly found the '011 prosecution history confirms that "intercepting" must be done by a shim. A26-27. In response to a rejection that included application claim 31 (which issued as claim 7 of the '011 patent), the patentee distinguished the prior art, stating:

> In other words, instead of just providing a socket that provides encryption services as in the Elgamel patent, ***the present invention inserts a shim between the sockets layer and applications programs that use the sockets layer***. The ***shim diverts function calls*** to an applications level encryption and authentication program….

A3609-3611 (emphasis added). Thus, the patentee made clear the invention of claim 7 is a shim that intercepts and diverts function calls, even though the claim does not recite a shim. SSL says this '011 history is irrelevant to the '796 patent, SSL Br. 42, but claim 7 of the '011 patent and claim 27 of the '796 patent use *identical* claim language for "intercepting." That the patentee's response to the rejection also addressed additional "concepts" (SSL Br. 42) does not undermine patentee's clear and unambiguous statement that "the present invention inserts a shim … [that] diverts function calls…." A3611.

3. SSL's Proposed Construction of "Intercepting" Violates the Plain Meaning and is Inconsistent with the Intrinsic Evidence

SSL's proposed construction for "intercepting" – as merely "receiving from a software module that which concerns another software module" (SSL Br. 44) should be rejected, first, because it defies the plain meaning of "intercepting." Merely "receiving" something is clearly not "intercepting," whether or not that something "concerns another." A postal worker "receives" a letter from the sender and postmarks it before sending it on to the recipient. The letter "concerns" another person; but if the letter is processed as intended, and delivered where intended, it is not "intercepted."

Second, SSL's construction relies on vague and indefinite terms that are inconsistent with the claim language. The claims do not refer to intercepting anything that "concerns another software module," much less shed light on what that might mean. Rather, the claim language is specific: what is intercepted is "function calls and requests for service" or a "destination address."

Third, SSL's construction is inconsistent with how the '796 patent distinguishes the prior art. In Figure 2, the function calls sent by peer-to-peer applications ***36*** and intended for the lower level drivers are received and processed by the socket (e.g., Winsock) **22**, before they are passed down to the lower level drivers, as intended. Even though Winsock "receives" a function call that

"concerns" another software module because it is intended for a lower level driver, it does not "intercept" that function call, but simply passes it on as intended. SSL's construction thus would read on what the patent describes as the prior art, when the patent distinguishes Figure 2 as *not* disclosing the invention.

4. Substantial Evidence at Trial Supported the Jury's Verdict, and Under Any Construction of "Intercepting" Based on the Intrinsic Evidence, Citrix's Products Still Would Not Infringe, So Any Error Was Harmless

Citrix adduced substantial evidence that the GoTos do not intercept and divert function calls/requests or a destination address, and that the software SSL accused of being a "shim" is in fact not a shim, as discussed above at 20. Again, SSL does not even attempt to dispute that, if the court's construction is correct, substantial evidence supports the non-infringement verdict.

Instead, SSL argues that it was prejudiced by "addition of the 'shim' and 'diverting" requirements." SSL Br. 42. But because the MeetingID, SessionID, and MachineNameKey are not "destination addresses," no reasonable juror could have concluded that the GoTos "***intercept[]*** a destination address," regardless of how "intercepting" is construed. In effect, if this Court affirms the district court's construction of "destination address," the construction of "intercepting" becomes a moot issue.

And again, SSL's alleged prejudice is premised entirely on this Court adopting ***SSL's*** construction of "intercepting" as merely "receiving from a software module that which concerns another module." SSL Br. 44. As noted earlier, such a construction is clearly incorrect.

Moreover, SSL cannot show prejudice because it does not articulate any facts in which "intercepting" function calls/requests in the GoTos actually occurs ***as claimed in claim 27***. Regardless of whether interception is done by a shim or whether it includes diverting, the claim language requires "interception" of particular types of commands – function calls and requests for service – as they proceed from the application to their intended destination, "a lower level set of communications drivers." A118(20:56-58). ***This does not happen in the GoTos.*** Rather, to initiate a communication over the Internet, the GoTo application programs "directly call Winsock." A2056-2058. Winsock receives function calls/requests that are directed to it, does only what it is called upon to do, and then passes the data to a lower level set of communications drivers. A2056-2059. From there, the communications go exactly where they are intended to go. A1878; A1892; A1898; A1904-1905; A2058-2065 ("when it's told to connect to the broker, it connects to the broker"); A2095-2096. No "intercepting" occurs anywhere, even if a shim and diversion are not required. A2052-2055.

Thus, even if the court's construction was incorrect, the error was harmless. No facts support the theory that software in the GoTos "intercepts" function calls/requests or destination addresses. As with "destination address," the only way SSL could even argue that "interception" occurs is by proposing a clearly improper claim construction.

C. The District Court's Construction Regarding The Step Order Was Correct, And The Verdict Was Supported By Substantial Evidence

SSL's third claim construction argument pertains only to GoToMyPC and GoToAssist. For these two services, the verdict should also be affirmed because the court correctly concluded the steps of claim 27 fall into four groups, and while the steps within a particular group need not be performed in a specific order, each of the steps within a group must be completed before the steps in a subsequent group. A13-14. The step order required by the court is spelled out in the final jury instructions and in a summary sheet given to the jury and included as an addendum to this brief. *See* A7413-7417; A2432-35. The court acknowledged that "[a]s a general rule, method claim steps are not construed to require a specific order." A13. But they should be so construed when, as here, "the steps actually recite or require, via grammar or logic, a specific order, or if the specification 'directly or implicitly requires such a narrow construction.'" A13 (quoting *Altiris v. Symantec*, 318 F.3d 1363, 1369-70 (Fed. Cir. 2003)).

SSL concedes that "[s]ome steps logically occur before others," SSL Br. 50, so the issues here are narrow. For example, SSL does not dispute that the Group I "intercepting" steps logically must come first. *See* A113(9:42-53) ("shim **50** operates by hooking or intercepting call initiation function calls"); A111-112(6:66-7:3). Rather, SSL alleges only two errors in the court's construction.

First, SSL argues the court erroneously required that files be encrypted before the second computer is contacted by the server. SSL Br. 50. In fact, because of an apparent drafting error, the claim repeats the "encrypt files" language in two different places, and as a result the court included "encrypt files" in both Group II and Group IV, on either side of the Group III step of "causing said server to communicate with the second of said two client computers." However, the specification, describing Figure 7, teaches that the encryption of files occurs *after* the server contacts the second client computer. A114(12:8-10, 12:18-19). But in any event, the question is moot, and any error with respect to this limitation is harmless, ***since SSL fails to identify any prejudice it suffered as a result of this alleged error.*** SSL Br. 51. Nor could it, since Citrix ***never argued*** that it did not infringe because encryption of files had to occur before the second computer is contacted by the server.

Next, SSL contends the "session key" generation portion of "causing" steps 27[C]/[E] in Group II need not occur before the server communicates with the

second client computer, and that SSL was prejudiced because Citrix demonstrated that this order was not met in GoToMyPC and GoToAssist. SSL Br. 50-51. SSL's argument should be rejected because the Court would have to rewrite the claim by splitting the "causing" step into pieces, with different parts of the step occurring at different times than what is recited in the claim, an approach this Court has previously rejected. *See Aerotel v. T-Mobile USA,* No. 2010-1179, 2010 WL 5376233 *2 (Fed. Cir. Dec. 20, 2010). Moreover, the second "causing" step logically *requires* communicating with the server to come before the session key is generated, as the communicating is done "***in order to enable*** the applications level authentication and encrypt program ***to generate said session key***." A119(21:3-6) (emphasis added).

SSL's proposal is also contrary to the specification. In the patent, the shim intercepts "call initiation function calls" in a first client computer, and "in response thereto," the software **20** in the first computer "initiates communications with the authentication server **23**, … in order to carry out the authentication protocol." A113(9:47-52). The "authentication protocol" includes session key generation. A109(2:28-32); A113(9:55-57). Thus, the patent teaches precisely what claim 27 requires —session key generation occurs ***after***, and in direct response to, "interception."

At trial, Dr. Smith provided "substantial evidence" to support the jury's verdict of no infringement of GoToMyPC and GoToAssist based on the district court's construction of this issue. A2129-2152. SSL does not dispute this. Accordingly, if this Court confirms that communicating with the server comes before generating the session key, the jury's verdict of non-infringement of GoToMyPC and GoToAssist should stand.

Even if the construction is not confirmed, any error would be harmless, since the evidence concerning "destination address" and "intercepting," overwhelmingly supports those grounds for non-infringement for GoToMyPC and GoToAssist, *independent* of any step order issue.

Moreover, Citrix also proved an *additional* way GoToMyPC and GoToAssist fail the required step order. SSL does not mention or challenge this additional ground on appeal. Specifically, in GoToMyPC and GoToAssist, the second client computer must communicate with the server (a Group III step) ***before*** the first client computer communicates with the server (a Group I step). For example, in GoToAssist, the customer at the second client computer starts the entire process by communicating with the server to post a help request in GoToAssist. Only ***after*** this communication can the server assign a SessionID and provide *it* to the expert's computer. A1893-1909, A2136-2149; A7129. Likewise, "in GoToMyPC, computer 2 must contact the server first before anything can

occur." A2130. This is backwards from the required step order, which requires the first client computer to "intercept" the destination address and then contact the server *to provide it* the destination address, thus enabling the server to communicate with the second computer. Because SSL does not challenge this part of the construction or this evidence as to GoToMyPC and GoToAssist, even if this Court agrees with SSL's two alleged errors above, those errors would be harmless.

D. If Any One Of The Claim Constructions Relevant To An Accused Product Is Upheld, The Verdict Should Be Affirmed

SSL's argument that this Court must remand if it disagrees with even one of the court's constructions is inconsistent with this Court's precedent. Cases such as *Ecolab, v. Paraclipse,* 285 F.3d 1362, 1373 (Fed. Cir. 2002), place the burden on SSL, the appellant, to show both an error in construction of a term, *and* that "the errors had prejudicial effect." SSL must prove that the different instruction could have led to a different *verdict* on infringement given the evidence as a whole. This is because, if "the same verdict would necessarily be reached absent the error … a new trial would be mere waste and affirmance of the judgment is required." *Id.* at 1374. Thus even if this Court finds errors in claim construction, it should affirm if "substantial evidence appears in the record supporting the jury's verdict and if correction of the errors in a jury instruction on claim construction would not have changed the result, given the evidence presented." *Teleflex,* 299 F.3d at 1328.

Under this Court's precedent, SSL cannot win a remand simply by identifying an error on *any one* claim construction issue and noting that the infringement question posed to the jury was a "general" one. Nothing in the "general verdict" cases SSL cites supports such a broad proposition. The general verdict cases state, unremarkably, that this Court should reverse when an error by the district court might have "tainted the verdict." *SEB S.A. v. Montgomery Ward & Co.*, 594 F.3d 1360, 1374 (Fed. Cir. 2010), *aff'd on other grounds*, 131 S.Ct. 2060 (2011).[2] But nothing in those cases relieves SSL of the burden of proving that correction of the error would have changed the ***verdict***, given the evidence at trial.

In *Verizon Services v. Cox Fibernet Virginia*, 602 F.3d 1324, 1342 (Fed. Cir. 2010), for example, when an appellant challenged the district court's claim construction on one issue, but there were other grounds for non-infringement independent of the challenged construction, this Court did not even examine the alleged error, and instead affirmed, stating: "Because the evidence that [defendant's] system does not practice several of the[] limitations does not depend on the disputed claim construction, the jury had substantial evidence to find that the [asserted] patent was not infringed *independently of the disputed limitation*." (Emphasis added). This Court did not even examine whether the jury's

[2] The "general verdict" discussion in *SEB* was pure dicta in any event, because this Court found no error in any theory presented to the jury. 594 F.3d at 1374.

consideration of the allegedly erroneous grounds might somehow have "tainted" the verdict or even whether in fact the jury relied on those other grounds for the non-infringement verdict.

SSL attempts to distinguish *Verizon* on the ground that *Verizon* cited another case, *Teleflex*, that SSL finds factually distinguishable. But what the *Verizon* court ***did*** was affirm the district court even when there might have been error in one claim construction, simply because there was substantial evidence of non-infringement based on other claim limitations. *Verizon* does exactly what SSL argues this Court cannot do.

And *Verizon* is nothing unusual. After amending a district court's claim construction this Court regularly considers "whether, on the correct instruction, the jury could have reached only one verdict," *On Demand Mach. v. Ingram Indus.,* 442 F.3d 1331, 1337 (Fed. Cir. 2006), because "the record on appeal supplies substantial evidence to support the jury verdict under the new claim construction." *Bowers*, 320 F.3d at 1334. Sometimes, as in *Verizon*, the Court concludes the jury's verdict would not have been altered by a new claim construction. And in other cases the Court concludes that a jury inevitably would have reached the *opposite* conclusion under the correct claim construction. *See, e.g., Exxon Chem. Patents, v. Lubrizol*, 64 F.3d 1553, 1561-62 (Fed. Cir. 1995); *Bowers*, 320 F.3d, at

1334. But there is simply no rule that every time this Court finds a claim construction error after a general verdict, a new trial is required.

In this case, SSL does not even attempt to meet its burden of showing ***the verdict*** would have been different if it convinces the Court of only ***one*** of its proposed constructions. As in *Verizon*, each of the three issues on appeal is independent, and the evidence supports the jury's verdict as to each issue independently.

For example, if the court's construction of "destination address" was correct, the jury necessarily would have reached the same non-infringement verdict for all the GoTos regardless of any error in the construction of "intercepting" or the order of steps. If the ID numbers SSL accused of being intercepted are ***not*** destination addresses, then the GoTos could not satisfy the "intercepting a destination address" limitation. And, SSL would also be left with no theory, and no evidence, that any of the GoTos satisfied the additional limitation of "transmitting the encrypted files directly to" the MeetingID, SessionID or MachineNameKey. The jury's verdict thus can and should be sustained solely on the "destination address" issue alone.

Likewise, if the court's construction of "intercepting" was correct, the jury would have reached the same verdict based on the substantial evidence that the GoTos did not use shims to intercept or divert, regardless of how the "destination address" issue is resolved.

Further, sustaining the district court's construction that certain steps must be performed in a certain order would likewise defeat infringement with respect to GoToMyPC and GoToAssist, independent of the other two issues. And, because Citrix never argued at trial that the step order was a reason to reject the infringement accusation against GoToMeeting, SSL certainly cannot show that any error in the court's instructions on step order affected the verdict with respect to GoToMeeting, since the jury verdict form specifically broke out the infringement question by the three individual accused GoTo services. A47-48.

E. SSL Is Not Entitled To Costs As A Prevailing Party

Finally, SSL argues it was the "prevailing party" under 35 U.S.C. § 285 and Fed.R.Civ.P. 54(d). The district court concluded that because both parties achieved some success and sustained some failure, neither was the prevailing party and thus each should bear its own costs. A62-63.

Even fully prevailing parties are not *entitled* to recover any costs; they are merely *eligible* to receive costs. In accord with that principle, this Court affirmed an identical order in *Ruiz v. A.B. Chance Co.*, treating the court's conclusion that neither party prevailed as a decision not to award costs. 234 F.3d 654, 670 (Fed. Cir. 2000). The Court should similarly affirm the court's conclusion here that SSL did not merit an award of costs. SSL did receive some relief, but Citrix received greater relief by winning on the primary '796 patent. Thus as in *Ruiz*, "neither

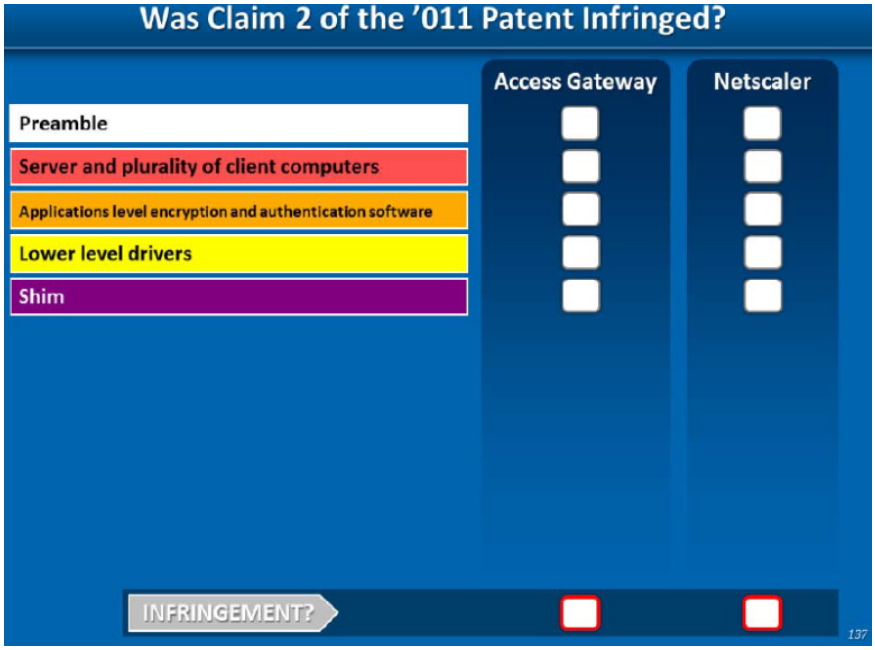
party prevailed sufficiently to require an award of costs" and the district court's "decision not to [award costs]" cannot be an abuse of discretion." *Id.*

II. THIS COURT SHOULD GRANT JMOL OR REMAND FOR A NEW TRIAL OF THE '011 PATENT CLAIMS

A. The District Court Should Have Granted A JMOL Of Non-Infringement Because Citrix's Evidence Showed That AG And Netscaler Do Not "Encrypt Files" And SSL Presented No Evidence On The "Encrypt Files" Limitation

On the '011 patent, the court's denial of Citrix's motion for a JMOL of non-infringement based on the "encrypt files limitation" was error. The jury's verdict is not supported by substantial evidence because the ***only*** evidence in the record is that Citrix did *not* meet the "encrypt files" limitation.

SSL chose to deliver Dr. Kelly's testimony on the '011 patent in a way that ignored the "encrypt files" limitation. Dr. Kelly testified that the claims contain "a lot of words," and "a lot of detail," so he relied on a chart that reduced the claim elements to "shorthand phrases" and addressed whether those phrases were met by AG and Netscaler. A1356-1357. For example, with respect to claim 2, Dr. Kelly briefly showed the jury a chart with the claim language. A1357; A7248. But when he gave his infringement analysis, he used the following summary chart from which "encrypt files" was omitted:



A1358; A7249. Dr. Kelly followed this procedure for each claim, never once referring to the "encrypt files" limitation. *See* A1358-1359; A7250-7252; A7255.

As a result, Dr. Kelley completely failed to discuss whether AG and Netscaler met the court's claim construction for "encrypt files." As noted above, the court ruled that "encrypting files is distinct from encrypting packets," "the encryption must occur at the file level," and encrypting files means "render[ing] a set of data used by a program unintelligible." A31-33. Additionally, all the claims further require that the files to be encrypted must be "sent by an application program" A134. Dr. Kelly gave no testimony on these concepts.

It is irrelevant that Dr. Kelly mentioned the concept of "encryption" when he pointed to a padlock icon on one document and stated: "You can see the padlock icon that … this is going to use encrypted communication." A1362-1363. He also

testified the accused products had "authentication and encryption software." A1364. But he ***never*** discussed the "encrypt files" limitation, how the software in the accused products performs encryption, or what he understood the encrypted unit to be.

Rather, the only record evidence confirms AG and Netscaler do not encrypt ***files***. Mr. Murgia testified: "Access Gateway doesn't encrypt files. Access Gateway operates at a – at a level below the file level, so what we see are generally packets." A1941-1942 (referring collectively to AG and Netscaler). Dr. Smith, likewise testified AG and Netscaler do not encrypt files, and so do not infringe. A2186, A2188-2190; A2195. SSL did not even cross-examine either witness on this issue. Thus, their testimony stands "uncontradicted and unimpeached," mandating JMOL of non-infringement in favor of Citrix. *Med. Care Am. v. Nat'l Union Fire Ins.,* 341 F.3d 415, 420 (Fed. Cir. 2003).

The court based its denial of Citrix's JMOL motion on irrelevant documents and testimony cobbled together by SSL after the trial, none of which Dr. Kelly ever connected to the "encrypt files" limitation. A83-84. For example, the court pointed to slides Dr. Kelly used for other limitations. *See* A1362-1364, A1367-1369; A7261; A7263; A7268. The court also cited Dr. Kelly's testimony that Internet Explorer is an "applications program." A1409. That has nothing to do

with whether AG and Netscaler encrypt ***files***, and was proffered during a discussion of the functionality ***of the GoTos***, not AG and Netscaler. A1403-1410.

None of the cited evidence satisfies SSL's burden to produce substantial evidence that AG and Netscaler "encrypt files." Citrix, in contrast, showed that they do not.

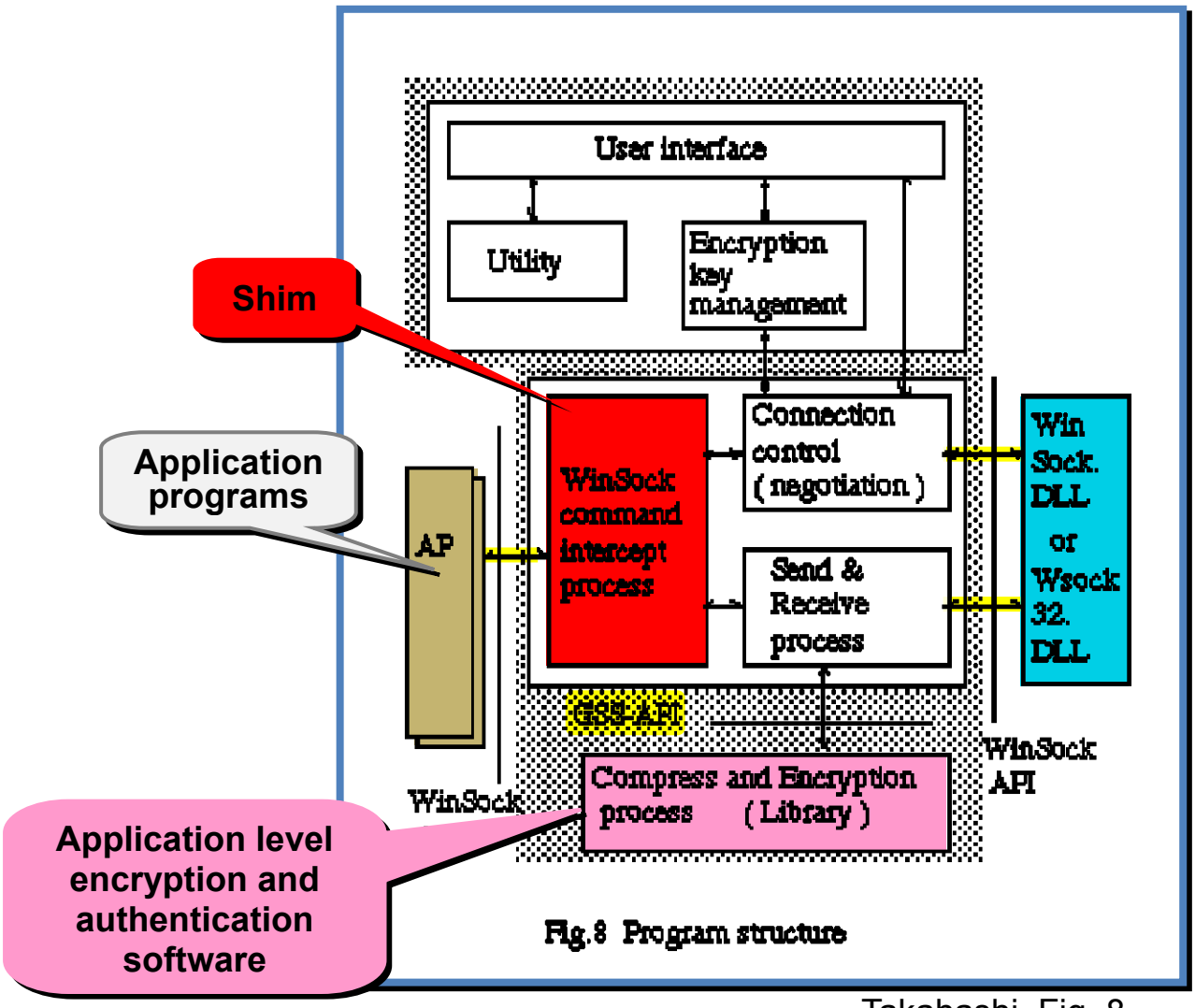
B. JMOL Of Obviousness Of Claims 2, 4 And 7 Should Have Been Granted When SSL's Expert Provided Only Conclusory Statements In Response To Citrix's Evidence Of Obviousness Based On Takahashi And RFC1508

JMOL should also have been granted on the ground the claims are obvious over Takahashi in view of RFC1508. SSL disputed only two points: (i) whether Takahashi discloses "applications level" authentication and encryption software, A2368-2371, and (ii) whether RFC1508 discloses "mutually authenticate the server and the client computer" in claims 2 and 4. A2370-2372. SSL never disputed Dr. Smith's testimony that it would be obvious to combine the two references, and that a POSA would be motivated to do so. A2179-2180.

Briefly, Takahashi teaches use of a "secure communication add-in program" that adds encryption capability to a mobile computing device without modifying existing application programs or the computer's network stack. A6865-6866(Figs. 1, 2); A6870(Fig. 8). Takahashi also adds a shim—called the "Winsock command intercept process"—between application programs and Winsock that intercepts function calls sent by an application program. A6866-6867 (discussing Fig. 2).

Takahashi teaches that intercepting function calls causes the "secure communication add-in program" to contact a server and generate a session key. Under "Negotiation function," Takahashi states: "In our negotiation sequence … selection of the encryption method, identification of the encryption key, etc., are done. … [F]irst the connect command from the application program is intercepted by our secure communication add-in program." A6867; *see also id.*(Fig. 3); A2179.

Key structures of the Takahashi's system identified by Dr. Smith are shown in Figure 8, with coloration and labeling added to match Dr. Smith's testimony. A6870; *see also* A2169-A2176; A6839-6841:



Takahashi, Fig. 8

The "Compress Process and Encryption" software, colored in purple, is the "application level" authentication and encryption program required by the claims, and includes a "set of software that is used for authentication and encryption." A2175-2176. Dr. Smith explained that "application level" means software that is "above the TDI layer." *Id.; see also* A123(Fig. 3). Takahashi also uses the GSS-

API–in yellow), which is the very API that is also discussed in RFC1508, so it was obvious to combine Takahashi with RFC1508. A2176-2177; A2179-2180.

Dr. Kelly's rebuttal testimony about Takahashi was cryptic and entirely conclusory. With respect to Takahashi's authentication/encryption software, he stated only, "Well, I disagree. With respect to the TDI layer, I disagree that this is an applications level program." A2367-2370. He provided no explanation of what he meant and no supporting facts.

His testimony, moreover, is directly inconsistent with how the '011 patent defines "applications level" software. The '011 claims track the "three basic layers" identified in the specification, from lowest to highest: "the first of which is the Network Driver Interface Specification (NDIS 3.0) layer, the second of which is called the Transport Driver Interface (TDI) layer, and the third being the file systems. ***These layers are generically referred to as the network driver layer, the transport or transport driver layer, and the applications layer.***" A128(2:59-65) (emphasis added). Thus, the patent defines software operating above the TDI layer as at the "applications level," as Dr. Smith testified. A2175-2176.

The patent also gives repeated examples confirming this definition of "applications level." The patent identifies HTTP, SMTP, and FTP as examples of "applications level" protocols, since these protocols "operate at the layer above the transport layer." A129(3:36-41). The patent also teaches that applications

programs use sockets such as Winsock as an interface between the applications level and the transport layer, and thus are above the transport layer. A129(3:42-56). And, the patent describes the prior art Smartgate software as "placed between the Winsock layer and the applications," and teaches that this positioning is at the "applications level." A129(4:8-11); A130(5:13-14).

Takahashi's secure communication add-in program is also installed above the transport layer between application programs and Winsock, and thus it too is at the applications level. A2171; A2176; A6866(Fig. 2). Dr. Kelly's unexplained "I disagree" cannot overcome the evidence from Takahashi and the '011 patent itself confirming that the Takahashi software is "applications level" software. *Krippelz v. Ford Motor Co.*, 667 F.3d 1261, 1269 (Fed. Cir. 2012) (conclusory testimony insufficient to defeat JMOL); *Regents v. AGA Medical*, 717 F.3d 929, 941 (Fed. Cir. 2013).

In any event, the requirement for installing security software at "the applications level" in a client/server VPN cannot be the basis for non-obviousness. The patent teaches that ***in the prior art*** "the preferred approach to implementing client/server virtual private networks is to use ***an applications level security system*** to encrypt files to be transmitted." A129(4:3-6)(emphasis added); A128(1:58-65); A131(7:49-51)(prior art Fig. 2). Thus, as Dr. Smith testified, installing authentication/encryption software at the "preferred" applications level in

Takahashi's client/server system would have been obvious. *See KSR Int'l v. Teleflex*, 550 U.S. 398, 417 (2007).

Finally, Dr. Kelly's assertion that RFC1508 does not disclose "mutual authentication" is directly inconsistent with RFC1508 itself. Without discussing the text of RFC1508 at all, Dr. Kelly stated, again in purely conclusory terms, that RFC1508 "provides none of the details that you would need in order to actually implement authentication." A2371-2372. RFC1508, however, specifically refers to "***authenticating a client to a server*** using elements carried within a single token, and of authenticating the server to the client ***(mutual authentication)*** with a single returned token." A6875 (emphasis added). In a series of paragraphs, RFC1508 describes how, in GSS-API, tokens are exchanged between client and server "so that mutual authentication is performed." A6875-6876. Takahashi itself teaches use of GSS-API, and thus, as Dr. Smith testified, "it would be obvious to one to actually use the GSS-API for mutually authenticating the server and client computer." A2180. Nor would it be difficult to do so, as the '011 specification itself states that the authentication schemes used in the patent "are already well known, and can be implemented as a matter of routine programming." A128(2:36-41).

C. SSL Failed To Satisfy Either Prong Of The Willfulness Standard, Because Citrix Had Objectively Reasonable Defenses And SSL Presented No Evidence Citrix Knew Of Or Should Have Known Of The Alleged Infringement Until After This Case Was Filed; The Court Also Erred In Excluding Evidence Of Citrix's Good Faith Belief In Its Defenses

The court also erred in denying Citrix's motion for JMOL against SSL's allegation of willful infringement. The court erred by finding that that "Citrix['s] alleged defenses … are not reasonable" and submitting willfulness to the jury, A2412-2413, and by denying JMOL after the jury's verdict, *see* A96-97. SSL had the burden of proving both "prongs" of the willfulness test by clear and convincing evidence. *Seagate,* 497 F.3d at 1368, 1371. Here, SSL's evidence fails both prongs.

1. Citrix's Non-infringement and Invalidity Defenses were Reasonable.

Citrix had well-founded defenses that AG and Netscaler did not infringe and the patents were invalid, including the arguments discussed above. A "reasonable litigant" could "reasonably expect" those defenses to succeed. *Bard*, 682 F.3d at 1008.

Tellingly, SSL never moved for summary judgment against any of Citrix's defenses, and when Citrix *did* move for summary judgment, SSL did not cross-move and the court did not reject Citrix's arguments as baseless, but instead found "genuine and disputed" factual issues on both non-infringement and invalidity.

A7294. Such a finding of genuine issues of material fact has been recognized by this Court as evidence a defendants' defenses were reasonable. *Lee v. Mike's Novelties,* 2013 WL 6097232 *6 (Fed. Cir. Nov. 21, 2013). That the jury ultimately found infringement "does not make the accused infringer's defenses objectively unreasonable." *Id.*

With respect to infringement, as discussed above, SSL's failure to adduce ***any*** evidence to contradict Citrix's evidence that AG and Netscaler do not "encrypt files" directly supports the objective reasonableness of Citrix's non-infringement defense. In denying Citrix's JMOL and finding Citrix's "encrypt files" defense unreasonable, the district court ignored Citrix's evidence and instead relied on an inaccurate synopsis of Dr. Kelly's supposed "extensive testimony" on this topic. The relied-upon portions of Dr. Kelly's testimony had nothing to do with whether AG or Netscaler "encrypts files," Instead, the erroneously court referred, *e.g.*, to "data flow or traffic from Applications … to a [lower level program] via a shim," A95-96. The court also cited SSL's reference to "Internet Explorer," but that application is not used at all in AG or Netscaler, and was discussed only in the context of '796 patent, for the GoTos. A96. None of this evidence referred to the "encrypt files" limitation.

Citrix's invalidity arguments, as well, were backed by expert testimony demonstrating that all three claims were anticipated or obvious. A2179-2186.

Indeed, the PTO itself rejected the asserted claims as obvious based on Takahashi and RFC1508. A6573-6582; *see* A6865-6921; A2161-2186. At the time of trial, the asserted claims stood rejected on this art. Citrix could not have acted recklessly in proceeding to trial on an invalidity theory that was supported by the PTO's rejection. And shortly ***after*** trial, the PTO issued a "final" rejection based again on Takahashi and RFC1508. A6605-6634.

While the PTO ultimately reversed itself months after the trial and confirmed the claims, the PTO's rejections highlight the reasonableness of Citrix's invalidity defense. Even when confirming the claims, the PTO implicitly acknowledged the issue was close by allowing the claims only because of "insufficient evidence" to conclude that Takahashi had an "applications level" program. A6735. Contrary to the district court's straw-man argument (A99), Citrix never contended that the mere fact of reexamination is "an absolute bar to willfulness"; rather, Citrix contended that the PTO's repeated rejections show the reasonableness of Citrix's invalidity defense.

In its post-trial order denying JMOL on willfulness, rather than determine whether a "reasonable litigant" could "reasonably expect" Citrix's invalidity defenses to succeed, the Court applied its own belief as to whether Citrix ***would*** ultimately prevail on its defenses, stating "the Court is not convinced that Citrix will ultimately prevail on its invalidity defense" and "the Court is of the considered

opinion that the asserted prior art references simply do not invalidate the '011 patent under any standard of review." A56-57; A98.

Applying the correct standard, a reasonable litigant would have reasonably expected Citrix's prior art defenses to succeed, ***even up to and including the time of trial***. The court gave no weight at all to the testimony of Dr. Smith on invalidity, or to the fact that PTO examiners had repeatedly looked at the same art as Citrix and issued rejections based on that art.

In short, because SSL failed to show by clear and convincing evidence that Citrix was "objectively reckless," the question of willfulness should not have been sent to the jury. *Powell v. Home Depot USA*, 663 F.3d 1221, 1236 (Fed. Cir. 2011).

2. SSL Did Not Present Evidence that Satisfied the Subjective Prong of Willful Infringement

SSL also failed to provide clear and convincing evidence that any risk of infringement was "either known or so obvious that it should have been known to" Citrix. *Seagate*, 497 F.3d at 1371. As summarized by the court in its JMOL opinion, SSL's evidence of "reckless disregard of the '011 patent" rested on two facts: (1) Citrix's Mr. Mangum knew of the '011 patent because it was listed on attachments to the 2000 and 2001 Distribution Agreements between Citrix and V-One; and (2) Mr. Mangum "failed to communicate [his] knowledge to anyone at Citrix." A99-100.

The court disregarded other critical facts that cut directly against any possible recklessness by Citrix, including: Mr. Mangum testified he did not recall ever analyzing or reviewing the '011 or '796 patents, or discussing them with anyone at Citrix or V-One. A1750-1551; A1791-1794. And Mr. Mangum left Citrix in April 2002, more than two years before Citrix acquired either AG or Netscaler in late 2004 and 2005. A1587-1588; A1742. ***Mr. Mangum thus had nothing whatsoever to do with AG or Netscaler.*** Neither SSL nor the court ever identified ***any*** facts that would have led Mr. Mangum to investigate the '011 patent as to ***any*** Citrix product, much less to suggest that others might want to investigate the '011 patent vis-à-vis products he had never heard of and that Citrix was not even selling when he left the company.

Moreover, SSL provided no evidence that any person at Citrix had knowledge of the '011 patent when Citrix acquired AG and Netscaler in 2004 and 2005, or at any time thereafter, until the amended complaint was filed in 2009. A1797. Nor did SSL provide any evidence of why Citrix should have investigated AG and Netscaler for potential infringement of the '011 patent when those products were independently developed by third-party companies, and there was no evidence those products copied V-One's designs. A54; A1709-1710; A1714-1716. Before SSL's amended complaint, neither V-One or SSL ever suggested to

Citrix in any way that AG or Netscaler could possibly infringe the '011 patent. A1138-1140; A1732-1734; A1229-1231.

In *Seagate*, this court "abandon[ed] the affirmative duty of care." 497 F.3d at 1371. Thus, Citrix's supposed failure to investigate whether AG and Netscaler infringed the '011 patent ***on these facts*** cannot rise to the level of recklessness sufficient to establish willful infringement. The district court's failure to grant JMOL should be reversed.

3. The Court Erred in Precluding Citrix from Presenting Evidence of its Good Faith Belief that it Did Not Infringe the '011 Patent and that the Claims Were Invalid

Even if this Court agrees Citrix's defenses were objectively unreasonable and that SSL presented triable issues of willfulness, the jury's verdict on willfulness cannot stand because the court prevented Citrix from presenting evidence that Citrix believed in good faith it had valid non-infringement and invalidity defenses. A1670-1672.

First, the court erred by precluding Mr. Murgia, Citrix's chief engineer and product architect in the group that includes AG and Netscaler, A1939, from testifying regarding Citrix's good-faith belief those products did not infringe. A1670-1672. Mr. Murgia, Citrix's Rule 30(b)(6) witness with respect to technical topics concerning those products, had direct involvement in the design of AG beginning in 2007. A1668-1672; A1941. His proffered testimony was directly

relevant to Citrix's alleged subjective willfulness, and should have been admitted. *Seagate*, 497 F.3d at 1371; *cf. DSU Med. v. JMS*, 471 F.3d 1293, 1306 (Fed. Cir. 2006).

Second, the court erred by precluding Citrix from referring in any way to the '011 reexamination that Citrix had researched and filed. The jury thus never heard about the nature and timing of the rejections issued by the PTO, nor was Citrix able to cross-examine SSL's witnesses about inconsistencies between what SSL said in litigation about the prior art and what SSL had said to the PTO concerning the same prior art. A6002-6003; A2073-2080. This evidence was timely proffered and directly relevant to subjective willfulness and to the merits of the invalidity issues. A1668-1672. *Cf. Commil USA v. Cisco Sys.,* 720 F.3d 1361, 1368-69 (Fed. Cir. 2013) (holding the district court erred in excluding evidence of defendant's good-faith belief that the patents were invalid as a defense to induced infringement).

The prejudice from the exclusion of such probative evidence justifies a new trial on willfulness. *See Davidson Oil Country Supply v. Klockner*, 908 F.2d 1238, 1245 (5th Cir. 1990).

D. The Court Abused Its Discretion In Allowing SSL's Damages Expert To Base His Royalty Opinion On Non-Patent "License And Distribution Agreements"

If this Court does not reverse the infringement verdict, this Court should grant a new trial on damages because the court erred in allowing SSL's damages expert to base his royalty rate upon the non-patent License and Distribution Agreements. *See* A1609-1610; A4843-4957. SSL did not meet its burden of proving the agreements were comparable to the non-exclusive, domestic patent license that would result from the hypothetical negotiation for either the '011 or '796 patents. *Lucent*, 580 F.3d at 1329; *Laserdynamics v. Quanta Computer*, 2011 WL 7563818 *2-3 (E.D. Tex. Jan. 7, 2011). "Similar" or "close to" comparable accepted by the district court is legally insufficient. *See Lucent*, 580 F.3d, at 1327-32; *Wordtech Sys., v. Integrated Networks Solutions*, 609 F.3d 1308, 1319-21 (Fed. Cir. 2010); *ResQNet.com, v. Lansa*, 594 F.3d 860, 869 (Fed. Cir. 2010).

The License and Distribution Agreements were admittedly "not a patent license." *See* A1145-1146; *see also* A1547; A1610. V-One supplied Citrix with the Smartgate software product, plus certain supporting services, ***but gave no patent license***. A4848-4850. The fact that an appendix referenced the '011 patent should be irrelevant, since Citrix was not licensed that patent, and SSL itself asserted the Smartgate product ***did not even embody the '011 patent.*** A7295.

The court abused its discretion in allowing SSL's expert to rely on these agreements for his damages opinion. The agreements were admittedly "not on all fours with the issues before us." A7356. But even beyond that, the agreements shed no light on the parties' tendencies in *patent* licensing. Nor do they establish the relevant competitive positions of the parties in the hypothetical negotiation because the first agreement was more than four years before the hypothetical negotiation date for the '011 patent (A2255-2256), when the parties, particularly V-One, were in different financial conditions. A2289-2290.

The expert's reliance on such non-comparable agreements prejudiced Citrix because they served only to confuse and mislead the jury. *See Utah Med. Prods. v. Graphic Controls*, 350 F.3d 1376, 1385-86 (Fed. Cir. 2003); *Laserdynamics,* 2011 WL 7563818 *9-11. As such, admission of this testimony was prejudicial error and grounds for a new trial on damages. *Med. Care Am.,* 341 F.3d at 420; *Smith v. Transworld Drilling*, 773 F.2d 610, 613(5th Cir. 1985).

E. The District Court Erred By Awarding SSL Prejudgment Interest For The 4.5 Years When It Delayed Before Asserting The '011 Patent

Finally, the district court here should not have awarded prejudgment interest for the 4.5 years that SSL delayed before asserting the '011 patent against Citrix. A patentee's delay in filing suit or giving notice of infringement is undue where it is "self-serving" and prejudices defendants by causing damages to "escalate."

Crystal Semiconductor v. TriTech Microelectronics Int'l, 246 F.3d 1336, 1361-62 (Fed. Cir. 2001). Courts have discretion to "limit prejudgment interest, or perhaps even deny it altogether, where the patent owner has been responsible for undue delay in prosecuting the lawsuit." *General Motors v. Devex*, 461 U.S. 648, 657 (1983).

Here, SSL had no excuse for its 4.5-year delay. Its predecessor V-One reviewed the competition and sent letters in late 2003 to a number of *other* companies in the market, giving notice of the '011 patent, but not Citrix. A1182; A6990-7013. SSL then purchased the patents in 2005 but chose to do ***nothing*** with the '011 patent. For 4.5 years it never once contacted Citrix about the '011 patent, even though AG and Netscaler were on sale and all pertinent information about the products was publicly available. A1229-1230; A5857-5882.

SSL's delay severely prejudiced Citrix by allowing damages to escalate as Citrix continued to sell its products without any notice of even potential infringement. The court penalized Citrix on top of that by awarding SSL an additional ***$4.5 million*** in prejudgment interest for the 4.5 years of delay. Prejudgment interest is not intended to compensate a litigant for its own delay. *Crystal,* 246 F.3d at 1362; *Orion IP v. Mercedes-Benz USA*, No. 6:05-CV-322, 2008 WL 8856865 *6 (E.D. Tex. Mar. 28, 2008). If the judgment is not reversed, prejudgment interest should run only from the filing of the amended complaint in May 2009.

CONCLUSION

Citrix requests this Court to affirm the judgment for Citrix on the '796 patent and reverse the judgment below on the '011 patent and enter judgment for Citrix, or remand for a new trial or modification of the judgment.

Respectfully submitted,

/S/ J. ANTHONY DOWNS
J. ANTHONY DOWNS
LANA S. SHIFERMAN
GOODWIN PROCTER LLP
53 State Street
Boston, MA 02109
(617) 570-1000

WILLIAM M. JAY
GOODWIN PROCTER LLP
901 New York Avenue, N.W.
Washington, DC 20001
(202) 346-4000

ERICA D. WILSON
DAVIS WRIGHT TREMAINE LLP
505 Montgomery Street, Suite 800
San Francisco, CA 94111-6533
(415) 276-6500

BLAIR MARTIN JACOBS
MCDERMOTT WILL & EMERY LLP
500 North Capitol Street, N.W.
Washington, DC 20001
(202) 756-8000

LEIGH JOHN MARTINSON
MCDERMOTT, WILL & EMERY LLP
28 State Street
Boston, MA 02109
(617) 535-4000

Counsel for Defendants-Cross Appellants
Citrix Systems, Inc. and Citrix Online LLC

December 23, 2013

United States Court of Appeals
for the Federal Circuit

SSL Services, LLC v. Citrix Systems, Inc., 2013-1419, 1420

CERTIFICATE OF SERVICE

I, Elissa Matias, being duly sworn according to law and being over the age of 18, upon my oath depose and say that:

Counsel Press was retained by GOODWIN PROCTER LLP, Attorneys for Cross Appellants to print this document. I am an employee of Counsel Press.

On **December 23, 2013** counsel for Cross Appellants has authorized me to electronically file the foregoing **INITIAL BRIEF OF DEFENDANTS – CROSS APPELLANTS CITRIX SYSTEMS, INC. AND CITRIX ONLINE LLC** with the Clerk of Court using the CM/ECF System, which will serve via e-mail notice of such filing to all counsel registered as CM/ECF users, including any of the following:

Megan S. Woodworth
(WoodworthM@dicksteinshapiro.com)
Thomas D. Anderson, Esq.
(AndersonT@dicksteinshapiro.com)
Robert L. Kinder
(KinderR@dicksteinshapiro.com)
DICKSTEIN SHAPIRO LLP
1825 Eye Street, N.W.
Washington, DC 20006

Katya S. Cronin
(katya.cronin@lw.com)
Gregory G. Garre
(gregory.garre@lw.com)
Adam Michael Greenfield
(adam.greenfield@lw.com)
Katherine Twomey
(katherine.twomey@lw.com)
LATHAM & WATKINS LLP
555 11th Street, N.W., Suite 1000
Washington, DC 20004

Paper copies will also be mailed to the above counsel at the time paper copies are sent to the Court.

Upon acceptance by the Court of the e-filed document, six paper copies will be filed with the Court, via Federal Express, within the time provided in the Court's rules.

December 23, 2013

/s/ Elissa Matias
Counsel Press

CERTIFICATE OF COMPLIANCE

I hereby certify that this Brief for Defendants – Cross Appellants Citrix Systems, Inc. and Citrix Online LLC complies with Fed. R. App. P. 28.1(e). The brief contains 16,367 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii) and Fed. Cir. R. 32(b). This brief complies with the typeface requirements of Fed. R. App. P. 28.1(e) and the type style requirements of Fed. R. App. P. 32(a)(6). The brief has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in 14-point, Times New Roman font.

Respectfully submitted,

/S/ J. ANTHONY DOWNS
J. ANTHONY DOWNS
GOODWIN PROCTER LLP
Counsel for Cross Appellants